UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA
Denkleiers • Leading Minds • Dikgopolo tša Dihlalefi

Designing an Interest-to-Function Career Alignment Model for Cybersecurity Professionals

by
Paul Wyatt Poteete
17409952

Submitted in fulfillment of the requirements for the degree
Doctor of Philosophy
Information Technology

in the
Department of Informatics
Faculty of Engineering, Built Environment and Information Technology
University of Pretoria
Pretoria
South Africa

Supervisor: Dr. Rennie Naidoo 25 November 2020

Declaration

I understand what plagiarism is and am aware of the University’s policy in this regard.

I declare that this dissertation/thesis is my own original work. Where other people’s work has been used (either from a printed source, Internet or any other source), this has been properly acknowledged and referenced in accordance with departmental requirements.

I have not used work previously produced by another student or any other person to hand in as my own.

I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

I declare that this is my unaided work and has not been submitted to another university for any degree.

Paul W. Poteete

Dedication

This research is dedicated to my wife, Holly, without whose help and encouragement, I could not have undertaken such an endeavor.

To my children, Luke and Lisa for their understanding during the long periods of my divided attention.

To Prof. Rennie Naidoo for his continuous guidance throughout the years of research.

To the entire faculty and staff at the University of Pretoria and Geneva College who worked directly and indirectly with me to complete this study, as well as all of the individuals around the world who participated in the research.

Finally, may the outcome of this research be for the betterment of humanity, as each individual is created in God's image for a time and purpose.

Abstract

Cybersecurity professionals are in high demand, but the definition of individual interests and the functions that comprise those roles is more complex than it may seem. In the face of a global shortage of cybersecurity professionals, and an often-difficult team dynamic around these individuals, in addition to a dramatic rise in cybercrime and security breaches, it is important to define and understand career success and career performance within an organization. This research uses a design science approach founded on a sociotechnical theoretical framework based on Information Technology (IT) turnover and Human Resources (HR) theories to analyze individual factors of job satisfaction and job performance for cybersecurity roles to design a cybersecurity interest to function career alignment model through the integration of prominent indicators of individual interest. This is accomplished using a mixed methods approach of surveys, interviews, and a focus group that are employed using various techniques of visual, descriptive, correlation, and thematic analysis. Two key findings within this research involves cybersecurity roles and functions and the ability to align an individual's personal interests to those roles. In the former case, cybersecurity roles are poorly defined and are prone to widespread ambiguity, requiring the design of a taxonomy of discrete functions for analysis. In the latter case, individual interests, as analyzed through popular individual profiling solutions are vague and largely irrelevant to cybersecurity professionals. This requires that individual interests be defined and applied to relevant industry functions to provide meaningful alignment to job satisfaction and job performance. Among the implications for IT Turnover Theory, is the refined attribution of individual interests within cybersecurity roles instead of a monolithic interpretation of cybersecurity professionals as a single factor. This is also true for the Intermediate Linkages Model as the job satisfaction-turnover relationship may be further refined to include industry-specific functions for cybersecurity functions and the specific interests of cybersecurity professionals. The implications for design science research could extend beyond the usage of standard guidelines, venturing into this study's process of using design challenges to illuminate hidden design principles. This challenge-principle relationship may provide additional insight to new or existing facets of reasoning. These new viewpoints may uncover otherwise excluded aspects that provide additional insight into this study or topics beyond. For cybersecurity and human resources practitioners, this study provides several implications beyond the foundation for career training for functional guidance. It provides an alternative viewpoint on organizational and departmental design for cybersecurity to business alignment to increase individual job satisfaction and ultimately improve organizational performance. Future research would result in deployed artifact instantiations that promotes general career direction for future and current cybersecurity personnel, while also providing additional guidance to organizations for the proper deployment of cybersecurity teams. Other research could include IT careers beyond cybersecurity to create a standardized method for the alignment of interests to career functions for the improvement of individual job satisfaction and overall organizational performance.

Keywords: Cybersecurity, Career Success, Interest-to-Function, Career Performance, Job Satisfaction, Design Science Research

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ADR	Action Design Research
CTO	Chief Technology Officer
CISA®	Certified Information Systems Auditor
CISM®	Certified Information Security Manager
CISO	Chief Information Security Officer
CISSP®	Certified Information Systems Security Professional
DSRPM	Design Science Research Process Model
DESRIST	Design Science Research in Information Systems and Technology
DP	Design Principle
DREPT	Design Relevant Explanatory/Predictive Theory
DSR	Design Science Research
DSRM	Design Science Research Methodology
EDT	Explanatory Design Theory
FFM	Five Factor Model
FJA	Functional Job Analysis
HR	Human Resources
ICCWS	International Conference on Cyber Warfare and Security
ICT	Information Communications Technology
IDGA	Institute for Defense and Government Advancement
IEC	International Electrotechnical Commission
IFS	Internal Field Separator
III	Individual Interest Inventory
IS	Information Systems
ISACA®	Information Systems Audit and Control Association
(ISC)^{2}®	International Information Systems Security Certification Consortium
ISDT	Information Science Design Theory

ISMS	Information Security Management Systems
ISO	International Organization for Standardization
IT	Information Technology
JVIS	Jackson Vocational Interest Survey
MBTI®	Myers-Briggs Psychometric Type Indicator
MySQL	Structured Query Language Database
PHP	Hypertext Preprocessor
SSL	Secure Socket Layer
MPS	Motivating Potential Score
NIST	National Institute of Standards and Technology
NCDA	National Career Development Association
NDA	Non-Disclosure Agreement
NICE	National Initiative for Cybersecurity Education
NIST	National Institute for Standards and Technology
O*NET	The Occupational Information Network
PII	Personally Identifiable Information
RIASEC	Realistic, Investigative, Artistic, Social, Enterprising and Conventional
SANS	SysAdmin, Audit, Network and Security
SCADA	Supervisory Control and Data Acquisition
SIOP	Society for Industrial and Organizational Psychology
SP	Special Publication
STS	Sociotechnical Systems
TfM	Tolerance for Monotony
WIN	Workforce Intelligence Network

1 Introduction

Cybersecurity roles and responsibilities are vast and range across a wide array of industries. The ability to determine the fundamental aspects of these roles and align those aspects with individual interests would create new methods for recommendations of organizational architecture, training courses, individual measurement, and further areas of research not visited in this study. This study focuses on the alignment of individual interests to specific cybersecurity career functions. This alignment provides measurements that may be used to promote specific cybersecurity tasks to specific individuals for gains in retention, performance, and satisfaction (Aruna & Anitha, 2015). Several academic and practitioner literary sources are reviewed in this investigation, allowing for a more comprehensive view of individual interests, career modeling, and cybersecurity functional roles.

1.1 Problem Definition and Scope

There is a global shortage of skilled cybersecurity staff facing organizations of every kind and location (Parker & Brown, 2019). The proper selection of a skilled and culturally competent employee is critical to the security and productivity of the organization (Brilingaitė et al., 2020). Recently, in "The Cybersecurity Workforce Gap," it is stated that by 2022 there could be over 1 million unfilled cybersecurity positions (Crumpler & Lewis, 2019). This is further exacerbated by the projections that the problem is not improving (Oltsik, 2019). These shortages are facilitated by more than economic and cultural factors; they are also influenced by inefficiencies in the lack of individual satisfaction created through the misalignment of personal preferences to cybersecurity functions (Oltsik, 2019). Included in the complexities of defining cybersecurity functions and staffing shortages, the proper alignment of individual interests to cybersecurity functions has an impact on more than the individual's well-being, it influences the overall organizational security and profitability (Park & Shaw, 2013). If consideration is taken to determine how well an individual may work in a complex security role, actions can be taken to maximize employee satisfaction and minimize organizational loss (Guzman & Stanton, 2009). It may be possible to produce these outcomes through an increased understanding of cybersecurity functions and individual preferences that directly related to those functions. Understanding both the organization's specific needs and the individual's preferences, quirks, and tendencies is critical to improving cybersecurity employee retention and organizational productivity (Aruna & Anitha, 2015).

Beyond staffing shortages, the alignment of individual interests to cybersecurity functions is complicated by other factors. New employees are generally not subjected to analysis of individual interests for cybersecurity role performance or retention objectives, and, cybersecurity functions are often poorly defined, leaving a lack of clarity to the operational definitions of the role. These issues are compounded by the complex nature of public and private organizational security requirements and the difficulty in adequate measurements regarding human preference factors. As opposed to psychometric testing, individual preferences must be assessed in accordance within the functional role to be fulfilled. Traditionally, several different psychometric instruments have been used by organizations to determine proper organizational fit, without regard to the specific tasks contained within the job (John et al., 2008; Petrides & McManus, 2004). This study will focus the analysis of several psychometric profiles that analyze a different aspect of individual effectiveness or satisfaction in a given set of organizational conditions. These psychometrics are used as a baseline for the development of a taxonomy of individual interests. The final integrated artifact aligns individual preferences to cybersecurity functions without involving psychometric testing. This will avoid the unnecessary inclusion of irrelevant data provided through generic psychometrics into the final artifact. This analysis of functional influences allows the study to narrow the infinite number of personality traits to a measurable quantity that can be correlated to individual security job functions. In this case, the attributes defined can be aligned with the myriad of specific cybersecurity functions that compose each individual role. Descriptions and analyses are provided for several psychometric profiling solutions, as well as the methods by which each model may be used as a basis for a non-psychometric preference analysis.

In regards to organizational complexity, long-term employment of individuals who both understand their function and understand the organization's specific culture and technical requirements is essential (Porter & Steers, 1973). The short-term introduction of cybersecurity staff performing what is thought to be non-critical, seemingly monotonous, functions, presents an immeasurable amount of risk to the organization. Due to the complexity within the fusion of technical and cybersecurity roles, an unknown amount of procedural function can become intuitive for the staff. The lack of, seemingly unnecessary, documentation for these repetitive tasks are often foundational to the proper security and operation of the firm; consequently, the physical or virtual outsourcing of these individuals to talent pools who's staffing changes on a day-to-day basis could be catastrophic (Kauffman & Josefek, 2003).

In the determination of relevant individual preferences, the proper alignment of preference to job functions within cybersecurity roles is unexplored or entirely neglected. To maintain these individuals, organizations must provide incentives that are appropriate to the unique nature of the work and each individual's set of unique preferences (McAfee, 2016). These incentives vary from simple monetary rewards to creative control over business-to-security alignment (Crumpler & Lewis, 2019; Francis & Ginsberg, 2016; Libicki et al., 2014). Although measurements and incentives beyond the alignment of individual interests to cybersecurity functions is outside the scope of this research, it is important for every organization to understand the often unique motivations and perceptions of success may vary widely for each cybersecurity staff member. This process can be achieved through careful analysis and alignment of motivating factors to cybersecurity functions. The final result will be an organization that increases productivity and satisfaction among cybersecurity staff. This research proposes that a work environment that aligns individual interests with functions for cybersecurity professionals is paramount to organizational success.

The scope of this research is limited to factors of individual alignment to specific cybersecurity functions. This is a necessary limitation, as the factors influencing satisfaction, performance, retention, and success are near infinite. For the inventory of personal interests to specific cybersecurity functions, qualifications such as training, ability, experience, or formal education are considered inclusive for all individuals who are working within a cybersecurity position. Management techniques, structures, and employee incentives are not evaluated on any scale, as these factors do not involve a taxonomy of individual interests or cybersecurity functions. Location, salary, coworker, politics, governmental system, and other extrinsic and intrinsic factors are also out of the scope for this study. This allows for the focused creation of a model that aligns individual interests with cybersecurity functions.

1.2 Problem Significance and Motivation

There is a worldwide lack of cybersecurity professionals. Beyond acquisition, cybersecurity employee retention is important to organizational stability and performance. This is especially true for individuals in roles that have ubiquitous access to the organization's critical systems. The employment of skilled cybersecurity professionals can provide peace-of-mind, or conversely, anxiety for management and organizational leadership (Bowen et al., 2006; Lunenburg, 2011). Existing in a non-traditional business environment, at no point in time do cybersecurity teams relax their stance regarding threats facing the organizational products or services (Kaelin, 2018). These threats originate from a chaotic mix of government, hacktivist, criminal, or mischievous sources on a timescale measured in nanoseconds (Libicki et al., 2014, Naidoo, 2020). Individuals in these roles are faced with a constant onslaught of criminal and malicious activity that may even originate, often unintentionally, from internal employees (Martini & Choo, 2014). Notwithstanding the particular personality characteristics originally possessed by the individuals employed in information technology or security, the authority and knowledge possessed by these individuals will influence their psychological state. This could be analogous to personal reflection among individuals working in law enforcement or in the midst of information with formal classifications of secret or above (Executive Office of the President of the U.S., 2009; Leggitt et al., 2011; The White House, 2018). These influences on individual preferences, and their resulting outcomes, must be considered for properly allocating individual positions.

There is also a level of anxiety related to the employment of the cybersecurity workforce (Francis & Ginsberg, 2016). This anxiety may be related to the complexity of cybersecurity roles and the lack of understanding of their respective function. Cybersecurity careers can be seen as being as broad and complex as those in healthcare, aeronautics, or any other diverse industry; however, there is little evidence in the literature that would indicate that this breadth and complexity is understood. The Cybersecurity Workforce Gap states that cybersecurity talent is hard to acquire (Crumpler & Lewis, 2019). These individuals have access to the most critical aspects of the organization and could easily bring operations to a crawl or catastrophic end. They present a flight risk, putting the security operations of the entire organization at risk of exploitation through both a loss of skilled resources and the potential for disgruntled retaliation (Naidoo, 2016). Their very existence within the organization is a calculated risk, but their absence would expose the organization to certain risk. Even so, there often exists an inclination to group all cybersecurity functions into a single role. This research enumerates and codifies cybersecurity functions into relevant categories. Beyond understanding the categorization of cybersecurity functions and the extent of individual interest on job satisfaction, organizations must learn to conduct thorough human resource analysis to only introduce individuals who are a proper fit for the culture and function of the organization (Bowen et al., 2006). This process can be lengthy and costly, consuming multiple hours from high-level management and skilled human resource representatives (Biggio & Cortese, 2013;

Colwill, 2009; Kauffman & Josefek, 2003). It is for good reason that organizations want to maintain safe and effective security operatives on their payrolls. A method to improve individual satisfaction and performance through aligning individual interests with cybersecurity functions would provide a solution, as well as the foundation for additional frameworks, for employee acquisition and retention. Without this alignment, the ambiguous incorporation of security functions into a poorly defined organizational structure is predicted to continue.

1.3 Methodology and Key Concepts

Using the Design Science Research Methodology (DSRM), three interrelated artifacts are developed to achieve the final goal of creating a career model centered on individual interests and job functions for cybersecurity staff. The Design Science Research Methodology (DSRM) involves the creation of a solution, called an artifact. Artifacts are the result of a design, build, and evaluate process (Hevner, 2007; Kuechler et al., 2004; Peffers et al., 2007). This may be conducted in a theoretical or real environment, but the instantiation of an artifact must accompany the DSRM process. When referring to the Design Science Research Process Model, a process of revision and evaluation is undertaken to repeatedly refine the established artifact. This is accomplished through the evaluation of literature, surveys, expert interviews, and focus groups, empirical data, and other methods that provide a broad scope of data to use for continued artifact revision and evaluation. Practitioner literature is considered alongside scientific and academic literature, as a supplemental resource for investigation. The disadvantage that practitioner literature does not involve the same level of scientific rigor as academic literature is a traded-off by the unique perspectives in the professional publication that may be otherwise absent within academic literature. There are also a number of peer-reviewed professional literary resources that are available outside of academic tradition. In the case of sociotechnical systems, especially those considered within the cybersecurity subdivision, practitioner resources are sometimes the only resources available. When considering individual interests or cybersecurity functions, as two independent prerequisite artifacts, it is important to understand their purpose in this study. An individual interest is a personal preference for an option within a set of defined options. In this study, the options are defined in regards to functions performed by cybersecurity professionals. This is different than a psychometric profile that analyzes a base set of personal motivations from a general psychological perspective. Cybersecurity functions are defined as those tasks performed by cybersecurity professionals on a regular basis, to exclude other common tasks shared by all employees. This allows for a set of specific tasks to be targeted for individual interests that only apply to a career in cybersecurity. The last artifact is an integrated artifact of the first two prerequisite artifacts, allowing for the creation of an alignment model. The third artifact is the primary solution proposed by this study.

1.4 Research Objectives

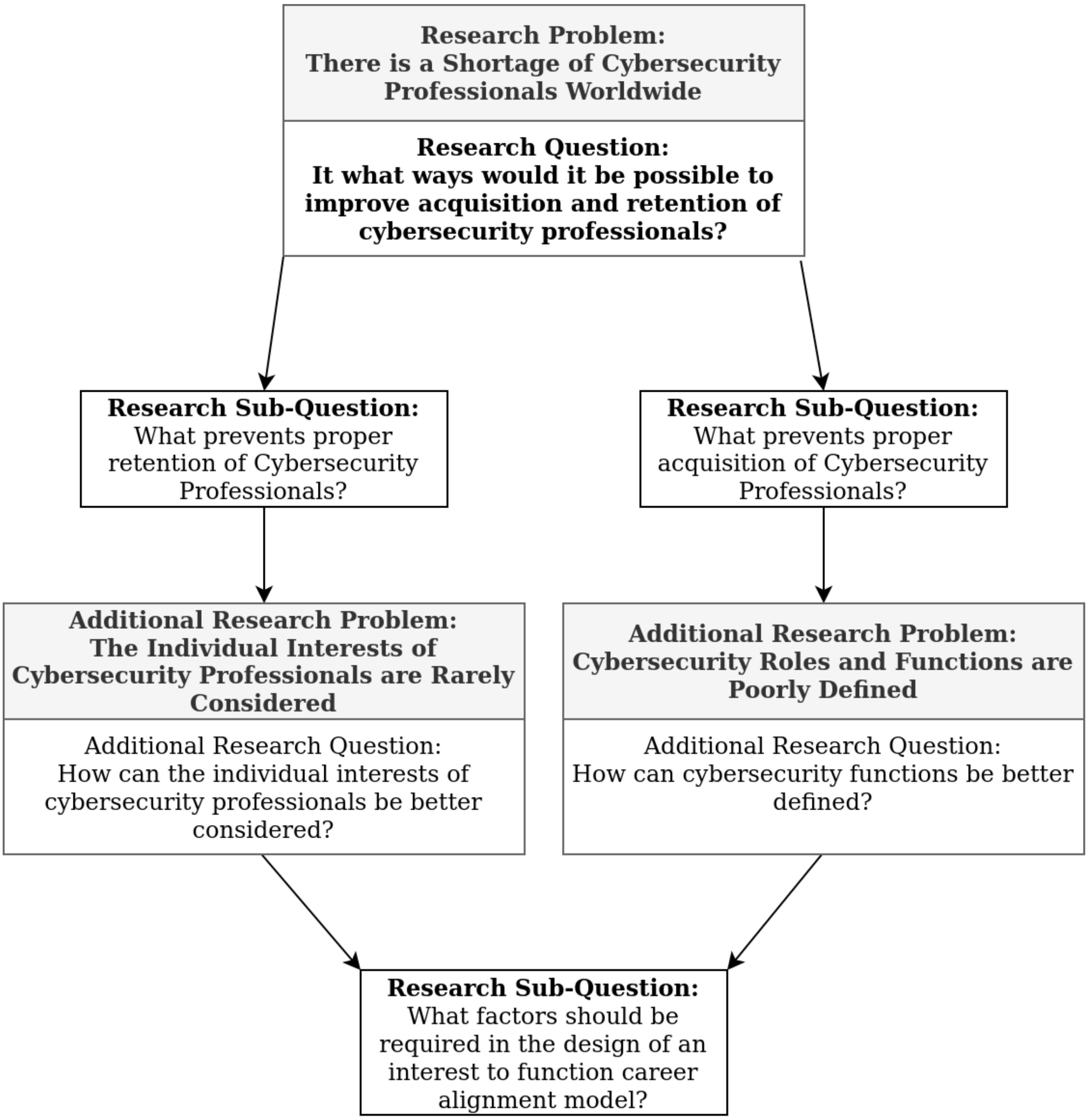
The primary problem identified in this study is the shortage of cybersecurity professionals worldwide. Through the initial and subsequent research questions, it is believed that the goal of this study will be to design a model that aligns individual interests and cybersecurity functions in such a way as to allow for the creation of a formulaic solution for both career-seekers and employers that predicts individual job satisfaction and performance. This is accomplished through the creation of artifacts that establish an association of personal preferences to career functions for the cybersecurity workforce, in such a way, as to allow the creation of a formulaic solution for both career-seekers, as well as employers that predicts individual job satisfaction and retention (Assante & Tobey, 2011).

The original research problem presented subsequent questions that generated additional sub-problems for this study. Each primary research question presented logical sub-questions that revealed additional problems of how to define a taxonomy of cybersecurity functions and how to create a taxonomy of interests for cybersecurity professionals as individuals. Due to the ambiguity in cybersecurity functional definitions and individual interests, these questions produced additional prerequisite research problems that are secondary to the original challenge regarding the shortage of cybersecurity professionals worldwide. This required an adjustment of the artifacts produced in this study to include two prerequisite artifacts for the single primary artifact. All of the problems, sub-problems, questions, and sub-questions eventually result in the final sub-question of how to align the interests and functions within the cybersecurity profession. This relationship is visualized in Figure 1-1 Research Problems, Questions, and Sub-Questions, and represented for the entire scope of this research study in Table 5-2 Research Problem, Questions, Propositions, Artifacts, and Design Principles Details in Chapter 5.

There should be a measurable alignment between personality preferences described in first artifact and job satisfaction experienced by employees serving in specific organizational cybersecurity roles (Hardigan et al., 2001; Hernandez & Johnson, 2014). The functions, motivating factors, business operations, leadership requirements, and human resourcing needs relating to cybersecurity concepts introduce a daunting challenge for researchers (Francis & Ginsberg, 2016). These factors interrelate across ambiguous individual predispositions and complex cybersecurity functions. The experience, training, and personal skills needed to research this confluence of topics are unusual. These factors, although elusive, are fundamental to the proper structure of a well-managed and effective cybersecurity program that protects those sheltered beneath it, while retaining those who provide it.

The need for this alignment is exacerbated by the reality that, throughout the world, there are reported shortages of skilled cybersecurity professionals (International Information System Security Certification Consortium (ISC)^2, 2018). This shortage costs businesses and governments economic, reputation, and other loss, through poor cybersecurity governance and protective controls. Although the shortage is facilitated by a number of identifiable economic and cultural factors, it is also influenced by the motivations of the individual who would be interested in a particular set of cybersecurity functions (Joseph et al., 2007). As the job functions are properly aligned with the respective individual personality preferences, capable staff will continuously fill a greater number of positions. The proper allocation of skills to the individual's motivating factors within the cybersecurity community will aid in the career satisfaction enjoyed by each member. This improvement may have a measurable effect on the number of skilled security candidates available at an international, national, and local level for organizations and governmental offices. Offices benefiting from this alignment will additionally be awarded with greater employee retention and performance.

Figure 1-1 Research Problems, Questions and Sub-Questions


Research Problem:
There is a Shortage of Cybersecurity Professionals Worldwide
Research Question:
It what ways would it be possible to improve acquisition and retention of cybersecurity professionals?
Research Sub-Question:
What prevents proper retention of Cybersecurity Professionals?
Research Sub-Question:
What prevents proper acquisition of Cybersecurity Professionals?
Additional Research Problem:
The Individual Interests of Cybersecurity Professionals are Rarely Considered
Additional Research Question:
How can the individual interests of cybersecurity professionals be better considered?
Additional Research Problem:
Cybersecurity Roles and Functions are Poorly Defined
Additional Research Question:
How can cybersecurity functions be better defined?
Research Sub-Question:
What factors should be required in the design of an interest to function career alignment model?

1.5 Theoretical and Practical Significance

This research investigates and provides solutions from both a scientific and practical standpoint. The output of this research should allow businesses to shape cybersecurity positions to maximize employee satisfaction and organizational performance. Individuals should be able to more clearly pursue cybersecurity career choices that more closely align to their individual interests. Scientific literature should be able to more correctly defined cybersecurity functions within roles and the interests that align with those roles, as aspects of both preference and performance, in relation to cybersecurity positions, are considered equally throughout this research, in their respective models (Biggio & Cortese, 2013). Consideration is taken to describe the proper alignment of personality preferences to specific position requirements, as this alignment has an impact on more than the individual's well-being, it influences how well that individual may work in different environments.

Employees within traditional business roles would consider the workplace to be an environment in which they can conduct their daily operations without the threat of constant criminal or malicious interruption. Often, these employees follow set standards of conduct and procedure, allowing for the efficient and effective management of the organization. Retention and performance methods for these individuals are commonly available, as they can be grouped into a normal distribution based on similarities within industries. This practice allows for ongoing operations to be conducted in a way that will meet a majority of employee needs (Colquitt et al., 2007). Employees who do not fit into the traditional model will be lost to attrition or endure the misalignment of the business to their individual needs.

Cybersecurity personnel deviate from traditional employees in both psychological idiosyncrasies and by the type of environment in which they are positioned. Cybersecurity personnel work within a virtual environment that is continuously hostile to their operations and the organization's productivity. Inexperienced and insufficiently educated cybersecurity personnel may negatively impact the organization through either mistakes or inappropriately constrictive or insufficient security controls (Dodge et al., 2012). The ongoing onslaught of chaos and innovative destructive forces facing the organization requires individuals of a particular personality and skill.

In both of these scenarios, employees are grouped into sociological segments that are impacted by job function, as related to their individual preferences. The striking difference between these roles could be the constant threat of malicious interruption within their individual positions. In reality, several jobs experience constant threats of violence or malicious actions (Sommestad et al., 2009). These jobs normally fall into industries such as law enforcement, the military, executive protection services, or other jobs where physical or technical threats are commonplace. Now, the virtual inter-connectivity of global entities has created an environment in which malicious attackers can originate within any vulnerable router or system residing within the organization. This has the effect of placing small aspects, of what was an industry familiar with threats, into the offices and cubicles alongside traditional workers. The requirement for cybersecurity professionals to work along with traditional employees has not created a new category; however, it has created the requirement for all industries to be more specific in their attribution of interest-to-function allocations for each employee. As the role and function of the individual has increased in complexity and variability within every industry, so must the alignment of job function to individual interests be re-imagined. As this model is developed, the artifacts will provide additional scientific basis for interest taxonomy and codification, as well as a taxonomy of fundamental cybersecurity functions. The alignment of these artifacts will assist individuals with future career planning and organizations with departmental associations or alignment.

1.6 Organization of the Study

Chapter 1 Introduction

This chapter introduces the challenge surrounding cybersecurity employment within an organization, the artifacts to be created, the IT turnover and human resources theories, and methodologies to be undertaken. This involves an introduction to the problem, motivation, and scope of the research with initial reference to its theoretical and practical significance.

Chapter 2 Design Science Research Methodology

Chapter 2 discusses the Design Science Research Methodology from its origin with Buckminster Fuller through its incorporation into information systems with recent discoveries by Venable, Pries-Heje, Baskerville, and Hevner (Baskerville et al., 2018; Hevner, 2007; Venable et al., 2012). Through the chapter, it becomes evident that rigor must be applied to all research. There is a focus on mixed methods using surveys, interviews, and a focus group for data collection. This includes visualization, thematic analysis, data frequency, and codification techniques in the analysis and evaluation of the data. The mixed methods approach allowed for several facets of the analysis to be undertaken in a complimentary effort.

Chapter 3 Literature Review - Problem Awareness

The literature review examines the various publications surrounding satisfaction, performance, evaluation modeling, psychometric foundations, career interest profiles, career retention theories, cybersecurity career foundations, cybersecurity functions, and interest inventories. Attention is given to methodologies for the measurement of individual interests and how interests are associated with career performance, satisfaction, and retention. This arrives at three key propositions. Each proposition provided data required for the next with the third defining an alignment between the prior two. First, a taxonomy of discrete job functions needed to be created for cybersecurity roles. Next, a taxonomy of individual interests that directly associate to the defined cybersecurity functions needed to be created. Finally, the third proposition aligns individual interests with cybersecurity functions to illuminate which functions most closely align with each individual interest.

Chapter 4 Design Principle and Artifact Development

Conceptual models are evaluated and defined to address the creation of three artifacts. The three artifacts are composed of two prerequisite artifacts required for the creation of a third integrated artifact: Prerequisite Artifact 01 - Cybersecurity Career Functions, Prerequisite Artifact 02 - Individual Interest Inventory (III), and the Integrated Artifact 03 - Interest-to-Function Alignment. Artifact 01 is a taxonomy of functions derived from a multitude resources composed of existing literature, organizational models, practitioner publication, and individual research. Artifact 02 creates a taxonomy of individual interests that was codified by accounting for only the interests that would apply to the functional cybersecurity categories from Artifact 01. Artifact 03 aligns the functional categories with individual interests to create an alignment model that is proportional for each interest and function. This includes detailed information regarding each stage of data acquisition and refinement needed to produce output that would be useful to the analysis and evaluation of artifacts 01 through 03. This also notes the determination of several design principles that arose during the research that should have further research outside of this study.

Chapter 5 Conclusion

Chapter 5 continues the discussion of the scope and limitations of this research, the intrinsic inability to precisely quantify every individual's desires and interests into specific career functions, and the imprecise nature of data when codified and reduced, which is required for it to become useful for analysis and evaluation. This chapter also revisits the purpose and opportunities presented through this research for individuals who wish to change careers or develop their skills for a cybersecurity career. This also includes reflections on this research and its impact to organizational success through the satisfaction and performance of its members, and the overall good that may come from individuals who are able to more effectively and efficiently direct their endeavors. This includes that the challenges of cybersecurity career guidance and employee retention are not easily addressed through any established literature or model. The problem of satisfactorily establishing organizational functions that align to individual employee interests is complex and needs to be better understood, and the developed model is a foundation for the continual development of this understanding.

Table 1-1 Organization of this Study shows my interpretation and method of displaying Design Science Research (DSR) within a sociotechnical framework. This does not elaborate on every aspect of the study but focuses on key points that are addressed throughout the research. This includes the chapter, overview, and key points in an easy to understand visualization.

Table 1-1 Organization of this Study

Chapter	Overview	Key Points/Ideas
1 **Introduction**	Introduce Research and Problem	• Design Science • Cybersecurity Careers • Individual Interests • Research Objectives and Questions • Research Sub-questions
2 **Methodology**	Approach to Solving Problem	• Design Science • Mixed Methods • Data Analysis
3 **Literature Review – Problem Awareness**	Problems and Challenges: Cybersecurity Careers, Individual Interests, and Alignment	• Academic and Practitioner Literature • Sociotechnical Framework • Artifact Development • Propositions: Taxonomy of Job Functions, Interests, and Alignment of Interests to Functions
4 **Design Principles**	Develop Three Artifacts	• Seven Design Principles • Design, Refine and Build Three Artifacts • Mixed Methods: Interviews, Focus Groups, Surveys • Data Analysis: Correlation Analysis, Visualization Technique, Thematic Analysis, Descriptive Statistics, Coding
5 **Conclusion**	Summary and Evaluation of Cybersecurity Interest-to-Function Alignment Model	• Contributions and Future Research Paths • Cybersecurity Career Retention • Individual Interests • Interest-to-Function Alignment • Design Science Research • Propositions • Design Principles

2 Methodology

2.1 Introduction

It may often be clear which philosophical paradigm would be most appropriate for a task, especially within certain well-established research methods. In the past, qualitative or quantitative approaches might automatically assign post-positivist or constructivist viewpoints on the nature of reality based on the causal relationships of their content (Orlikowski & Baroudi, 1991). In this age of technical development and the exponential increase in the accessibility of knowledge, there are often additional facets that may become apparent during the research process itself. Previously, only a limited number of viewpoints may have been feasible. Today, the intricacies of methodology may be further dissected to make unseen opportunities become clear. This is not to say that viewpoints cannot be fluid across several disciplines; however, well-established paradigms are often seen through a traditional lens.

2.2 Philosophical Bases of Design Science Research

As mentioned, a philosophical approach is often predetermined within well-established academic communities; however, within the pre-paradigmatic nature of information systems, philosophical underpinnings must be considered more rigorously (Vaishnavi et al., 2004/2017). This may be more true in Design Science Research, as the philosophical purpose in views of reality and meaning are continuously shaped by the design process and the iterations of the artifacts therein (Holmström et al., 2009). This is contrary to well-established paradigms of research that possess several volumes of work that provide philosophical mandates. In design science, within the sphere of technological advancements that extend beyond the observable, these foundations are limited or nonexistent (Vaishnavi et al., 2004/2017). This begins to lead DSR to a pragmatic viewpoint based on the design, instantiation, and refocus based on the efficacy of the instantiation. One's personal interpretation of any particular experience is relative to their own psyche. Individual interests may be profiled to an extent through categorical interest surveys. These analyses, albeit limited to a particular industry within a predefined set of interests, may provide measurements that can be quantified into each individual's relative experiences (Aken, 2001). These newly quantifiable interests may then be associated with experiences encountered while engaged in specific job functions, insomuch, as these functions can be categorized into a coherent taxonomy. The resulting quantification of individual interests may be aligned with the functional categories to provide a model of interest-to-function recommendations that would both improve individual satisfaction as well as organizational performance.

2.2.1 Different Research Paradigms in Information Systems

As applied to the purpose of this research through the identification of individual interests that align to cybersecurity functions to increase individual satisfaction and organizational performance to provide greater retention in the face of a shortage of cybersecurity professionals worldwide, individual experiences are pragmatically interpreted as relative to that individual's variable interests, which may be measured based on predefined interest categories that relate to cybersecurity career functions. This is not to say that all research within design science or information systems would follow a pragmatist approach. Depending on the nature of the research, the technological aspect could benefit from a positivist, post-positivist, or constructivist paradigm. Information systems' research that involves the production of a technological product could certainly follow a positivist or post-positivist paradigm of truth and the discovery of knowledge. In the same way, information systems may also include investigations into the human experience that require a growing understanding of what truths may be evident from a particular point of view (Mingers, 2001).

2.2.2 Ontology, Axiology, Epistemology, and Methodology

This research generally follows a realist ontology within a pragmatic paradigm that seeks verifiable artifacts that can be defined, developed, and evaluated; however, in some cases of human influence and interest, a relativist ontology is appropriate. In this case, philosophical viewpoints are marginalized where actual empirical evidence is available, and re-incorporated in cases of individual affection or bias. Due to decades of personal history within information systems, management, military operations, and cybersecurity, an emic approach to epistemology is essentially assumed. This positions this research from within, emic, to the community under research, not external, or etic, to the community. This also allows for the axiology to take a personal note, as the values that drive this research are centered around the improvement of organizational productivity and individual satisfaction. That both the employee and employer may find improvements in the quality of their lives based on the outcomes of this research.

2.3 Design Science Research Approach

2.3.1 Design Science Research Framework

DSR sets as its goal to solve a problem or modify a system or process to achieve alternative outputs (Vaishnavi & Kuechler, 2008). Whether this challenge is past, current, predicted, or imaginary, DSR needs to delve into the intricacies of each aspect to produce a new design and model that can be evaluated for its ability to meet the challenge. The process by which the model is developed is of academic value, as well as the building, and evaluation of the solution is of value to the body of science. This innate need to create a new system or process that will overcome a challenge is what sets DSR apart from other methodologies (Winter, 2008). In addition to the myriad of advantages provided by the design science research methodology (DSRM), Information Systems (IS) is able to benefit from new innovations within increasing human-system social integration (Peffers et al., 2007).

DSRM provides IS with an innovative way to conduct scientific research that involves social solutions to problems (Peffers et al., 2007; Vaishnavi & Kuechler, 2015). The requirements of post-war reconstruction were met by innovative new ways to use emerging technologies to solve civil engineering and new social interactions. Even through its success, Peffers explains that in the 1970's when the IS field began, there was a limitation to their acceptance into respected research journals (Peffers et al., 2018). It is now widely accepted that design science research provides a respectable method of producing good research, analysis, and repeatable results that are easily understood (Hevner, 2007). The popularity of design science research within the information systems field has increased over the years with a plethora of DSR publications at conferences and within research articles surrounding information systems publications (Deng et al., 2017; Hevner & Chatterjee, 2010; Peffers et al., 2018). Many published influential papers have popularized DSR, and this method can now be found in many respectable journals. Furthermore, the creation of an international design science research conference for technology, Design Science Research in Information Systems and Technology (DESRIST) began in 2006 (Hevner & Chatterjee, 2010). The first DESRIST conference was held in Claremont, California in 2006 and have continued yearly (Design Science Research in Information Systems and Technology (DESRIST), 2015).

The creativity allowed within the methodology is especially significant for the innovation concepts that are developed. DSRM provides a framework that lends itself to novel artifact development that is useful when designing new approaches to cybersecurity (B. Kuechler & Vaishnavi, 2008). This is notably significant as cybersecurity defensive and offensive controls often follow an unusual path when solving problems. DSRM is also useful in the punctual creation of new capabilities through artifacts that could be used to address the myriad of cybersecurity-centric challenges that arise moment by moment. The recent trend shows that Information Systems researchers have gravitated towards DSRM in recent years, especially those with a vision and a desire to make a global impact with their knowledge (Thuan et al., 2019). This integration of information system expertise and vision allows researchers the ability to promote and investigate their designs in a measured and consistent manner (Iivari, 2005; March & Storey, 2008).

2.3.2 Artifacts in DSR

Artifacts are the creations developed throughout the DSR process. They represent the solution to the problem or the tact that is applied to the challenge. Artifacts are also what sets DSR apart from other methodologies. In some cases, the design theory may overshadow the creation of artifacts; however, the artifacts still remain the output of the theoretical process (Gregor & Hevner, 2013). In qualitative and quantitative research, artifacts represent environmental or other conditions that feed into the research (Myers, 2013). In the case of DSR, artifacts are the creative output of the design process instead of the observed environment. Fuller originally coined the term artifact to represent the creative invention that was the result of design science research (Bayazit, 2004; Fuller, 1963; Peffers et al., 2018). He rated the efficacy of the artifact on its ability to solve a problem, not on monetary gain (Fuller, 1983). This origination of design science was for the betterment of society. As a historically-rooted philosophical foundation, design science research would be conducted to improve society for those who dwell in it.

Design Science Research Cycle

In order to construct creative artifacts that contribute to the body of scientific knowledge and follow the scientific method, several processes have been proposed in the forms of research cycles (Offermann et al., 2009; Vaishnavi et al., 2004/2017). These cycles all follow some method of acknowledgment of a problem, design of a solution, instantiation of an artifact, and evaluation of the artifact. The problem should be an issue that has no currently adequate solution or to which a new novel approach would provide a better solution. This novel solution would be the artifact portion of the design science research process. The next step would involve the design or planning of the artifact, followed by the actual creation of the artifact itself. In the next phase of the cycle, the artifact is evaluated through data collection mechanisms appropriate to its problem. At this point, the created artifact may be refined to better solve the problem or concluded as a success or failure within the scientific body of knowledge. In each of these steps, there should be some contribution to the body of knowledge (Gregor & Jones, 2007; Walls et al., 1992). In cases where the artifacts are proven to be ultimately ineffective, the rigor of the scientific process and evaluation through data collection should provide other researchers with foundational knowledge of the previous attempts.

2.3.3 Activities in Design Science Research

In order to conduct design science research, there must be a problem and an invention (Baskerville & Pries-Heje, 2010; Simon, 1969/1996). If left to chaotic practices of repetitive attempts and poor documentation, the solution, if ever achieved, would not constitute an artifact in design science research, as it would have failed to properly contributed to the scientific body of knowledge through poor documentation, preparation, and evaluation. Design science research activities involve that the problem be understood, that theories about a solution be investigated, the an instantiation be created and evaluated through artificial and, where possible, naturalistic methods (Venable et al., 2016). This involves the careful documentation of the theories and concepts, the creation of a solution, the evaluation of the solution through simulations and case studies, and the final settlement on the artifact's efficacy (Hevner et al., 2004).

2.3.4 Design Science Research Reference

In this research, many of the seminal design science research concepts and frameworks are compiled in Table 2-1 Key DSR Concepts and Relevant Aspects. This allows for a better understanding of the scientific underpinnings of the methodology used within this research to support revision and replication of processes, as well as, the fundamental guidelines that were analyzed. These works offer insight into new methodologies for various uses. Through the analysis of the many variations within DSR, one is able to infer some of the challenges within DSRM that these researchers were attempting to overcome in their specific use cases.

Table 2-1 Key DSR Concepts and Relevant Aspects

Key DSR Framework / Concept	**Relevant Aspects of Concept**
Comprehensive Anticipatory Design Science (Fuller, 1957)	Design science, artifacts
The Design Method (Gregory, 1966)	Foundational design science, design science defined
Design Science (Simon, 1969/1996)	Foundational design science concepts, scientific approach
Multimethodological Approach to Information Systems Research (Nunamaker et al., 1990)	Multimethodology approach, Design science research in IS
Information System Design Theory (ISDT) (Walls et al., 1992)	Design science in IS, behavioural science theory
Proposed Design Science Research Framework (March & Smith, 1995)	Design science research in IS
Seven Design Science Research Guidelines for Information Systems Researchers (Hevner et al., 2004)	Seven guidelines for DS research and evaluation
Design Science Research Process Model (DSR Cycle) (Vaishnavi et al., 2004/2017)	DSR Cycle, DSR philosophical purpose
Information Science Design Theory (ISDT) (Gregor & Jones, 2007)	Foundational design science concepts
Design Science Research Methodology (DSRM) (Peffers et al., 2007)	Artifacts and DSRM in IS
A Three Cycle View (Hevner, 2007)	Three cycles in design science
Proposed Research Process (Offermann et al., 2009)	Design science research process in IS
Explanatory Design Theory (EDT) (Baskerville & Pries-Heje, 2010)	Foundational design science concepts
Action Design Research (ADR) (Sein et al., 2011)	Design science for IS, artifact
Design Relevant Explanatory/Predictive Theory (DREPT) (W. Kuechler & Vaishnavi, 2012)	Design science research and theory in IS

Key DSR Framework / Concept	Relevant Aspects of Concept
Design Science Research Knowledge Contribution Framework (Gregor & Hevner, 2013)	Artifacts
Five Design Science Research Genres (Peffers et al., 2018)	DSR publications in IS

Note. The DSR Frameworks listed provide a historical overview of DSR as well as relevant aspects of several important concepts used in this research.

2.4 Data Collection for the Problem Awareness, Build and Evaluation Phases

Data collection took several turns. Initially, the challenges facing cybersecurity professional acquisition and retention was sighted as important factor through several practitioner resources (Creswell, 2009). A literature review of acquisition and retention models that were associated with cybersecurity and other industries was conducted to better understand the problem (Okoli & Schabram, 2010; Webster & Watson, 2002). It was determined that an artifact that aligned individual interests to cybersecurity functions would potentially provide an improvement for the employee acquisition and retention challenge. In order to create a model that aligned interests-to-functions for cybersecurity professionals, it was discovered that prerequisite artifacts would be needed before the creation of an integrated artifact would be possible. This led to the review and categorization of cybersecurity titles, individual interests, and cybersecurity functions within roles (see Table 2-2 Literature and Data Correlation to Artifacts).

Table 2-2 Literature and Data Collection Correlation to Artifacts

	Artifact 01 Cybersecurity Job Functions	Artifact 02 Individual Interests	Artifact 03 Alignment of Interests-to-Function
Literature	yes	yes	yes
Expert Interview: Part 1	yes	yes	--

	Artifact 01 **Cybersecurity Job Functions**	**Artifact 02** **Individual Interests**	**Artifact 03** **Alignment of Interests-to-Function**
Expert Interview: Part 2	yes	yes	--
Confirmatory Individual Interviews	--	--	yes
Focus Group	yes	yes	yes
Job Functions Survey	yes	--	--
Cybersecurity Interest-to-Function Survey	yes	yes	yes
Cybersecurity Interest-to-Function Online Questionnaire Final Survey	--	--	yes

2.4.1 Practitioner Organizations

Several practitioner frameworks within the cybersecurity industry were investigated to discover the most common job titles and functions in use (see Table 2-3 Key Practitioner Publications and Purpose) and (Table 2-4 Professional Documentation). Over fifty pages from the ISO 27000 Series, and hundreds of pages from the NIST and NIST/NICE series were used to define, compare, and contrast cybersecurity positions. In a continuing effort to better define cybersecurity functions, professional membership organizations were also researched. Primarily, ISACA® and (ISC)^2® were selected to provide additional details of cybersecurity roles and functions through their databases and professional literature. The final three practitioner resources were cybersecurity training organizations, employment databases, and cybersecurity industry websites. Practitioner or professional publications were used for much of the problem awareness phase of data collection (Sørensen et al., 1996). These resources allowed for an up-to-date view of what challenges individuals and organizations were facing in regard to cybersecurity hiring and retention. This is consistent with much of design science research that involves topics that have not been addressed from a formal academic viewpoint. This allows this study to use socially relevant research materials that have a direct impact on the human condition when addressing individual satisfaction and organizational challenges with cybersecurity roles. Articles were selected based on their relevance to the cybersecurity industry and individual interest profiles. The employment database and website resources provided comparative and contrasting viewpoints on the workforce categories from frameworks and training organizations, such as NIST SP800-181, to alternative opinions in The Occupational Information Network (O*NET) employment database from the United States Department of Labor (Sørensen et al., 1996). This included military operational websites that further supported an organization of cybersecurity functions into three categories of operational, defensive, and offensive functions. All of these resources were useful in continuously refining the roles and functions that would be encountered within a cybersecurity career for transition from cybersecurity job roles and titles to specific functions and tasks (Mayring, 2020). Through these resources, it was discovered that the thousands of cybersecurity titles and functions had very little consistency with actual tasks or functions. The resulting ambiguity in a majority of the titles led to the determination that titles and roles were in adequate to be used to represent specific functions in the interest-to-function cybersecurity alignment model. Functions would need to be further refined.

Table 2-3 Key Practitioner Publications and Purpose

Key Practitioner Publications	Purpose for Inclusion
<u>**Formal Frameworks**</u>	
NIST / NICE National Institute for Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) (Newhouse et al., 2017) **The ISO27000 Series International Organization for Standardization (ISO)** (ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2014)	The 50 publications in the ISO27000 series and the hundreds of pages from the NIST / NICE Special Publications were used to define, research, compare, and assess cybersecurity job titles.

Key Practitioner Publications	**Purpose for Inclusion**
Professional Organizations **International Information Systems Security Certification Consortium (ISC)^2®** (International Information System Security Certification Consortium (ISC)^2, 2019) **ISACA®** Information Systems Audit and Control Association (Otero, 2018)	The information from the Professional organizations (ISC)^2® and ISACA® were used to refine the cybersecurity job titles.
Training Organizations **The SANS Institute SysAdmin, Audit, Network and Security** (SANS) Institute (Paller, 2020) **InfoSec Institute Information Security (InfoSec) Institute** (InfoSec Institute, 2020)	These training organizations were used to further refine cybersecurity job titles.
Occupational Database **The Occupational Information Network (O*NET) Program** (Lewis & Rivkin, 2000) **Cybersecurity Career Websites** (Curran, 2016; *Cyber Security Degrees and Careers*, n.d.; *Cybersec Jobs*, n.d.; *Top 10 Security Careers*, n.d.; Department of Computer Science, n.d.; Doyle, 2019; Kaelin, 2018; Morgan, 2016; Security Wizardry, 2018; Zeltser & Hoyt, 2015)	The Occupational databases and cybersecurity career websites were used to compare and refine cybersecurity job titles.

Table 2-4 Professional Documentation

Organization	Title	Publication	Estimated Number of Pages / Publications
International Organization for **Standardization (ISO)** **International Electrotechnical Commission (IEC)**	Information Security Management Systems (ISMS) ISMS Family of Technology Standards	ISO 27000 (ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2018) ISO 27000 Family of approximately 50 Publications	50 Publications
National Institute of Standards and Technology (NIST) **National Initiative for Cybersecurity Education (NICE)**	The NICE Cybersecurity Workforce Framework	Publication 800-181 (Newhouse et al., 2017)	135 pages
	Security and Privacy Controls for Federal Information Systems and Organizations	Publication 800-53 (National Institute of Standards and Technology (NIST), 2020)	464 pages
	Information Security Handbook: A Guide for Managers	Publication 800-100 (Bowen et al., 2006)	137 pages
	Assessing Security and Privacy Controls in Federal Information Systems and Organizations	Publication 800-53A (Joint Task Force Transformation Initiative, 2014)	487 pages
	Managing information security risk: organization, mission, and information system view	Publication 800-39 (Locke & Gallagher, 2011)	88 pages
	Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories	Publication 800-60, II (Stine et al., 2008)	304 pages
	Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories	Publication 800-60, I (Stine et al., 2002)	53 pages

2.4.2 Theoretical Literature Review for Career Management

A multitude of academic resources for retention, employee acquisition, interest profiling, and modeling were available and useful to this study. This includes the resources in Table 2-5 Key Theoretical Publications used in Literature and Purpose. In the cases of the Role Conflict and Role Ambiguity, Role Theory, and Taxonomy Development in Information Systems, their function was to define working roles in general terms for general, as well as information systems, careers, respectively. In this research, this helped to refine cybersecurity career functions.

2.4.3 Theoretical Literature Review for Personality and Interest Profiles

Resources surrounding individual interests, personality profiles, and vocational influences were also identified in Table 2-5 Key Theoretical Publications used in Literature and Purpose. This research aided in the study of concepts related to individual motivation, employee retention, satisfaction, the measurement of individual traits, and employee relationships to organizations and careers that help determine significant individual interests as the basis for defining general terms and concepts for career interests. The psychometric analyses were useful in the initial integrated artifact development that revealed alignment of individual interests to career functions.

Table 2-5 Key Theoretical Publications used in Literature and Purpose

Key Publications used in Literature	Purpose for Inclusion
Role Conflict and Role Ambiguity (Johnson & Stinson, 1975; Rizzo et al., 1970)	Theories and Concepts used to refine Cybersecurity Career Interests.
Role Theory (Biddle, 1986; Katz & Kahn, 1978)	
Taxonomy Development in Information Systems (Nickerson et al., 2009, 2010)	
Agency Theory (Jensen & Meckling, 1976; Mitnick, 1976)	Theories and Concepts used to refine Cybersecurity Career Interests.
Gati's Model (Gati et al., 1996)	
Met Expectations (Porter & Steers, 1973)	
Self-Determination (Deci & Ryan, 2008)	
Taxonomy of Vocational Interests (Jackson et al., 1984)	
Unfolding Model (Lee & Mitchell, 1994)	Theories and Concepts used to refine Cybersecurity Career Interests.
Withdrawal Model (Hulin, 1991)	
Job Characteristics Model (Hackman & Oldham, 1976)	
Five Factor Model (FFM) (Digman, 1990)	Several psychometric concepts used to refine Cybersecurity Interests.
Jung Typology (Jung, 1921)	
Holland Vocational Interest Inventory (RIASEC) (Holland, 1986)	

2.4.4 Global Survey

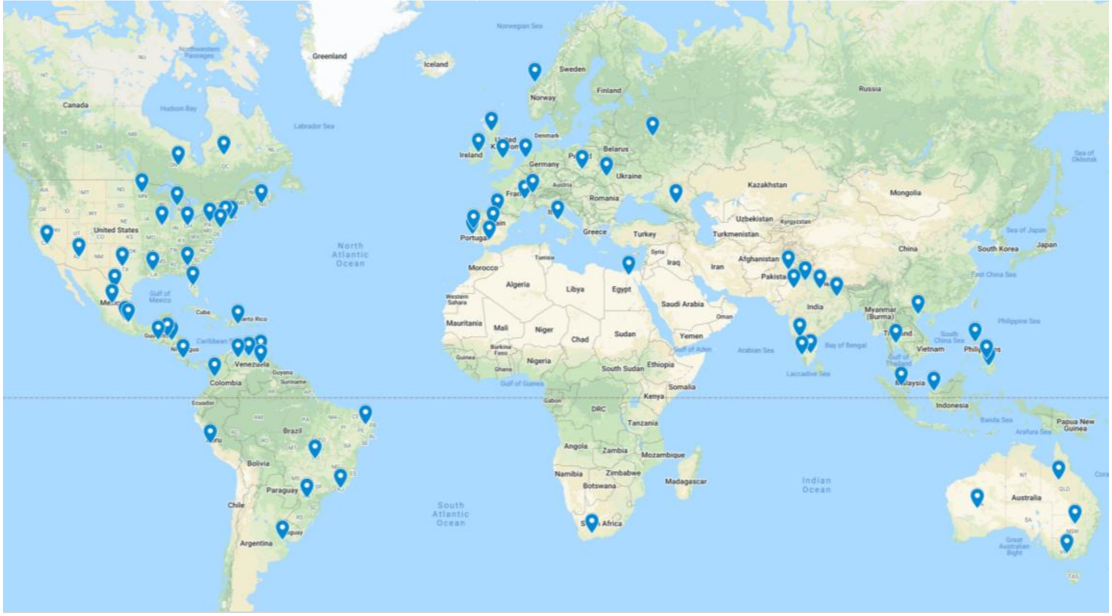
Survey Instrument Construction

There were a total of three online surveys created for specific purposes in this research entitled, Job Functions Survey, Cybersecurity Interest-to-Function Survey, and Cybersecurity Interest-to-Function Online Questionnaire Final Survey (see Table 2-6 Survey Demographic Details) (Evans & Mathur, 2005; Selm & Jankowski, 2006). The survey questions consisted of structured multiple choice, drop down lists, large matrix-type multiple selection, and a few open ended questions. The surveys were used to evaluate, design, and re-design the three artifacts in this research. Two surveys were conducted on a small sample group in order to test and refine the final questionnaire. The first survey is entitled Job Functions Survey (see Appendix C.6 Job Functions Survey Questions), and later a second survey was conducted entitled Cybersecurity Interest-to-Function Survey (see Appendix C.8. Cybersecurity Interest-to-Function Survey Questions). The primary method of data collection was the final online questionnaire (see Appendix C.9. Final Survey Questions) (see Figure 2-1 Map of Respondent Locations for Final Survey). Participation in the surveys as well as all of the data collection was completely voluntary.

Table 2-6 Survey Demographic Details

Survey	Online	Number of Participants	Respondent Locations	Respondent Titles
Job Functions Survey	Yes	7 anonymous	USA	Cybersecurity students
Cybersecurity Interest-to-Function Survey	Yes	5 anonymous	South Africa United Kingdom UAE USA Singapore	• Cybersecurity Student • Client Engineer • Trainee • Security Instructor
Cybersecurity Interest-to-Function Online Questionnaire Final Survey	Yes	155 anonymous	Worldwide (See Map Figure 2-1)	• Chief Technical Officers • Chief Financial Officers • Executives • Directors • President/CEO • Technical Staff • Senior Management • others

Figure 2-1 Map of Respondent Locations for Final Survey



Note. Map created with Google Maps data 2020

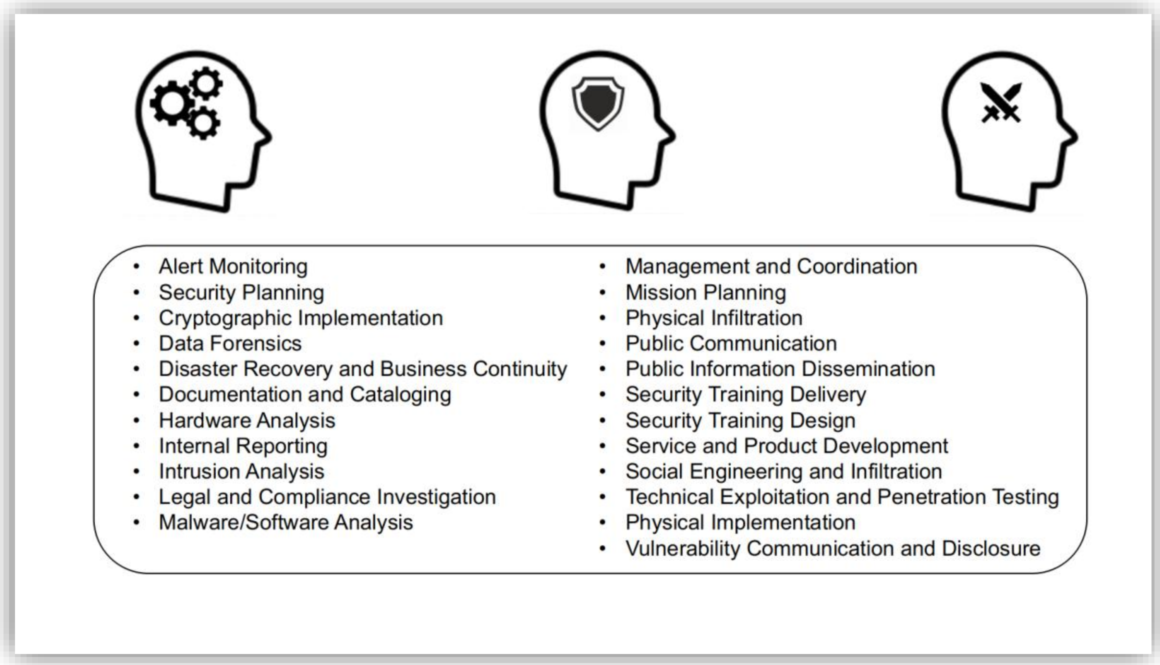
Job Functions Survey

One of the goals of this short, three question, survey was to determine the correlation between the job functions and the employees' individual interests

Eligibility

Participants were required to have a cybersecurity job function to participate in the Cybersecurity Interest-to-Function Surveys. The following graphic, Figure 2-2 Survey Function Graphic, was used in the surveys to display the cybersecurity job functions required for the survey.

Figure 2-2 Survey Function Graphic



- Alert Monitoring
- Security Planning
- Cryptographic Implementation
- Data Forensics
- Disaster Recovery and Business Continuity
- Documentation and Cataloging
- Hardware Analysis
- Internal Reporting
- Intrusion Analysis
- Legal and Compliance Investigation
- Malware/Software Analysis
- Management and Coordination
- Mission Planning
- Physical Infiltration
- Public Communication
- Public Information Dissemination
- Security Training Delivery
- Security Training Design
- Service and Product Development
- Social Engineering and Infiltration
- Technical Exploitation and Penetration Testing
- Physical Implementation
- Vulnerability Communication and Disclosure

Cybersecurity-related Experience

There was a total of seven anonymous participants who completed the Cybersecurity Interest-to-Function Survey. Two participants in this survey expressed that their job functions do not relate to the cybersecurity job functions listed in the first question; therefore, they were not eligible to continue the survey. Also, in this survey, participants shared the number of years in cybersecurity-related experience (Table 2-7 Cybersecurity Interest-to-Function Survey Participant Experience).

Table 2-7 Cybersecurity Interest-to-Function Survey Participant Experience

Number of Participants	Percentage	Years Experience
2	40%	10 or more years
1	20%	5-10 years
1	20%	1-5 years
1	20%	Less than one year

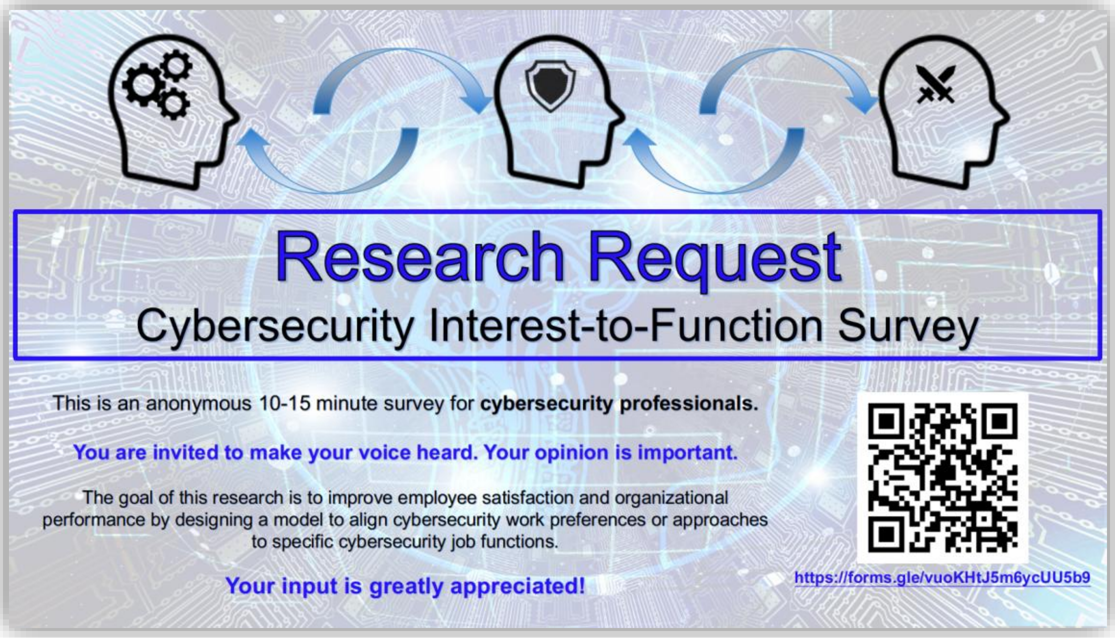
Cybersecurity Interest-to-Function Online Questionnaire Survey

The goal of the questionnaire was to determine the alignment of individual interests to cybersecurity functions. This was conducted through prerequisite requirements regarding the individual's career and experience. The candidate was then requested to complete the survey for common interests that are associated with career functions with which that individual is familiar.

Survey Distribution Methods

A research request graphic was created, Figure 2-3 Survey Invitation Example, to advertise the Cybersecurity Interest-to-Function Survey. A QR Code was created for this advertisement, allowing the survey to be quickly accessed.

Figure 2-3 Survey Invitation Example



Research Request

Cybersecurity Interest-to-Function Survey

This is an anonymous 10-15 minute survey for **cybersecurity professionals.**

You are invited to make your voice heard. Your opinion is important.

The goal of this research is to improve employee satisfaction and organizational performance by designing a model to align cybersecurity work preferences or approaches to specific cybersecurity job functions.

Your input is greatly appreciated!

https://forms.gle/vuoKHtJ5m6ycUU5b9

This invitation was advertised on several of my personal and professional social media outlets including: LinkedIn, Twitter, Facebook, Reddit, and Instagram. Several popular hashtags including: #cybersecurity #survey #cyberthreats #cloudsecurity #hacker #infosec #security #cyber #tech #gdpr #opensource #cybercrime #iot #informationsecurity #cybersecurityawareness #datasecurity were determined and utilized. Several research organizations saw the research posts and re-shared the advertisement to their groups. This survey was also advertised on two professional community online forums for cybersecurity professionals.

2.4.5 Focus Group

Table 2-8 Focus Group Participants

Number of Participants	Respondent Location	Respondent Job Title
5	Pennsylvania, USA Wellington, New Zealand	• Managing Director, Large International IT Consulting Organization • CEO, Technology Consulting Organization • Technology Services Professionals

Focus Group Goals

There were a total of five participants in the online focus group (Stewart & Williams, 2005; Tiene, 2000). They were all selected because they are working in cybersecurity careers (Table 2-8 Focus Group Participants).

The focus groups were identical to scope and purpose of the initial interview questions (see Appendix C.7. Focus Group Questions). The only variation was that all of the respondents could see and comment on each other's statements anonymously. Focus groups of cybersecurity professionals is one of the secondary measuring instruments (D. L. Morgan, 1996). The focus group responses were used in the evaluation of the three artifacts in this research study. Slides were used to assist in the guidance and clarity of purpose for the research (see Appendix C.2 Focus Group Slides).

Focus Group Protocol Instruction

An online discussion board forum was created to allow invited participants to anonymously, safely and securely contribute and respond to the research questions by simply going to CyberBridge.me/forum, which is on a website that I personally host at Amazon.

A Linux-based forum bulletin board software called phpBB was used, downloaded and modified it for this research. Although, the PHP coding language is identified through the initialism's current meaning of "Hypertext Preprocessor," its origins are made more clear by the humble original meaning, "Personal Home Page." The BB in phpBB stands for "Bulletin Board.

Focus Group Protocol Construction

The following is a brief overview of the steps used to create the bulletin board forum.

Step 1. Researched Discussion Boards

Step 2: Install a MySQL Server

```
 apt-get install mysql-server mysql-utilities mysql-common
```

Step 3: Install PHP

```
  apt-get install --install-recommends -y php php-mysql php-common php-gd php-curl php-mbstring php-xml php-xmlrpc php-soap php-intl php-zip
```

Step 4: Install Modules for Apache (MySQL, PHP, SSL)

```
  apt-get install libapache2-mod-php php-mysql unzip
```

Step 5: Install phpBB3:

```
  https://www.phpbb.com/downloads/

  cd /var/www/
  mv html html.original
  wget https://download.phpbb.com/pub/release/3.3/3.3.0/phpBB-3.3.0.zip
  unzip phpBB-3.3.0.zip
  mv phpBB3 html
  cd html
  chmod 666 config.php
  mysql
  create database phpbb3;
  grant all privileges on phpbb3.* to sql_user@localhost identified by 'password';
  exit;
```

Step 6: Configure phpBB3

Visit your public DNS Name and choose "install"

Step 7: After Installation:

```
  sudo -s
  cd /var/www/html
  chmod 644 config.php
  mv install /var/www/
```

Step 8. Created Admin Accounts

An administrator account was created and used the Administrator Control Panel and User Control Board to make setting changes.

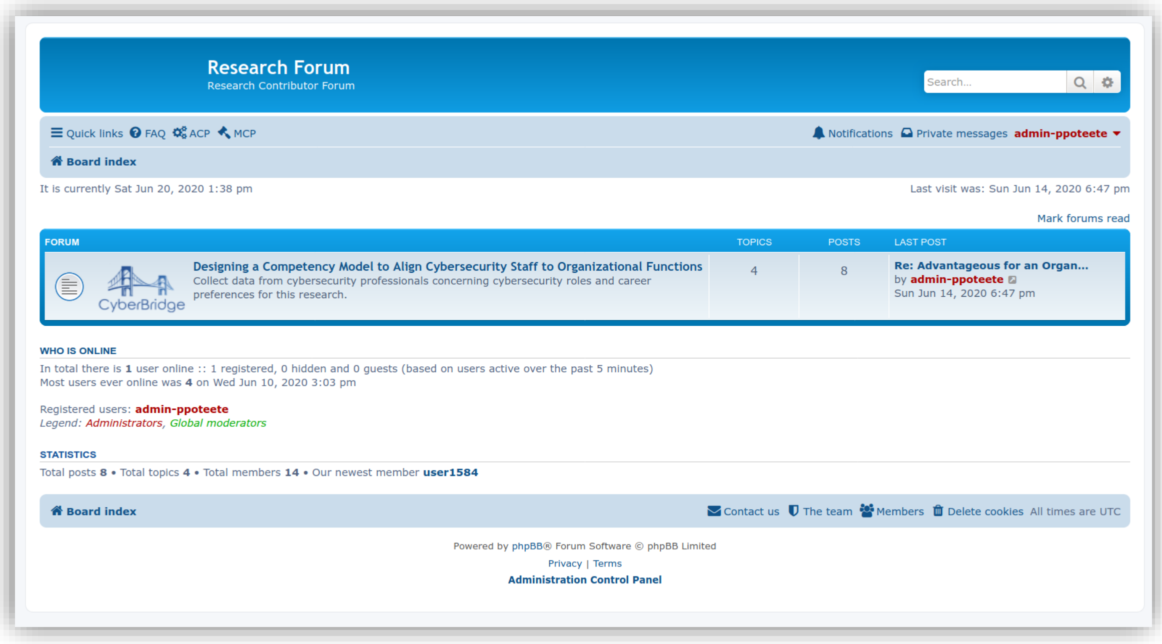
Step 9. Usernames

Anonymous usernames were created for each focus group participant. Each participant was also given a password to login securely.
Usernames:
user9848
user8843
user7698
user7927
user1385

Step 10. Questions
The discussion questions were typed in the forum and gave permissions to allow the users to post a reply. Several test accounts were created to check the settings before the focus group began.

The figure below, Figure 2-4 Focus Group Forum, is a screenshot of how the forum appeared.

Figure 2-4 Focus Group Forum



It is currently Sat Jun 20, 2020 1:38 pm

Last visit was: Sun Jun 14, 2020 6:47 pm

FORUM	TOPICS	POSTS	LAST POST
Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions Collect data from cybersecurity professionals concerning cybersecurity roles and career preferences for this research.	4	8	**Re: Advantageous for an Organ...** by **admin-ppoteete** Sun Jun 14, 2020 6:47 pm

WHO IS ONLINE

In total there is **1** user online :: 1 registered, 0 hidden and 0 guests (based on users active over the past 5 minutes)
Most users ever online was **4** on Wed Jun 10, 2020 3:03 pm

Registered users: **admin-ppoteete**
Legend: Administrators, Global moderators

STATISTICS

Total posts **8** • Total topics **4** • Total members **14** • Our newest member **user1584**

All times are UTC

Powered by phpBB® Forum Software © phpBB Limited

2.4.6 Expert Interviews

The Expert interviews were held online using online forms and email communications as well as one in-person interview (Cooke & McDonald, 1986; Myers & Newman, 2007). A total of seven individuals were chosen for the interview based on their positions and cybersecurity knowledge that they could contribute to this research (see Table 2-9 Interview Participant Details). Each individual was made aware that the interview results are anonymous, and that some basic personal information was collected for ethics verification (question 1). The interview participants were required to read and accept the informed consent and the Non-Disclosure Agreement (NDA) before beginning the interview (question 2). Expert interviews were used in the evaluation of the propositions and artifacts in this research. The interviews had several open-ended questions as well as a few selection questions. In the initial interviews, slides were used to assist in the guidance and clarity of purpose for the research (see Appendix C.1 Interview Slides).

Table 2-9 Interview Participant Details

Online	Number of Participants	Interviewee Locations	Respondent Job Titles
Online and In-person	7	Pennsylvania, USA Wellington, New Zealand Hawaii, USA	• IT Director, Large International Retail Business • Managing Director, Large International IT Consulting Organization • CEO, Technology Consulting Organization • Technology Services Professionals

Interviews (Technology and Security Founders)

The interviews were used to gauge the perceived validity of this research to organizations. In reality, the interviews presented much more information regarding the target audience potential for Artifact 03 - Interest-to-Function Alignment. It became clear that 1) the need to create an organically self-designed organizational structure for security operations and 2) the ability to aligning employees to a previously undefined structure was of great interest. In two occasions these topics were independently (not guided) presented to be of great use to candidate questionnaires and organizational restructuring. The excitement that was expressed in discussing the possibilities was greatly appreciated; however, that particular point of conversion would be best suited for additional research, as it was out of scope for this particular study.

Interview Participants

One confirmatory interview was held at a mutually convenient location. A manager in cybersecurity at an organization in the United States with 20 years of cybersecurity experience was interviewed. Another confirmatory interview was online using ZOOM. A managing director of a large information security organization was interviewed (Bogner & Menz, 2009).

The Expert Interviews (Interview Part 1, Interview Part 2, and Google Forms)

The Expert interviews were intended to provide insight into gaps in the artifact structure and contents; however, they were useful in also determining the proper sequence and structure of the questions. During the first round of interviews, it was discovered that some of the career functions in Artifact 01 and individual interests in Artifact 02 presented issues with ambiguity and clarity. To correct for these findings, a second wave of interviews and Google forms were constructed to better identify challenges (see Appendix C.4 Expert Interview Questions - Part 2). After making the requisite changes in terminology and achieving a satisfactory state, the interview materials were scripted to the primary survey.

Several short welcome videos were created on YouTube to welcome the participants, introduce the research, and explain the format of the questions. A sample of the video with a chart in the screen can be seen in Appendix C.3 Participant Welcome Video.

Online Data Collection

Current limitations for physical access of the respondents did not impact this research in a negative manner. It would appear that the current pandemic situation, COVID-19, may have increased the respondents willingness to join via video conferencing, social media messengers (Chen & Neo, 2019), and shared reciprocal video clips. The ability to perform both synchronous and asynchronous communications for the research allowed the avoidance of issues regarding time zones, pandemic restrictions, and even some language barriers, as some respondents were able to use online translation tools to better understand the questions in their own language. In order to promote responses, study and use of tools with which the respondent was most familiar was required. This prevented the respondent from needing to learn additional tools to comment on this research, reducing the barriers to responses.

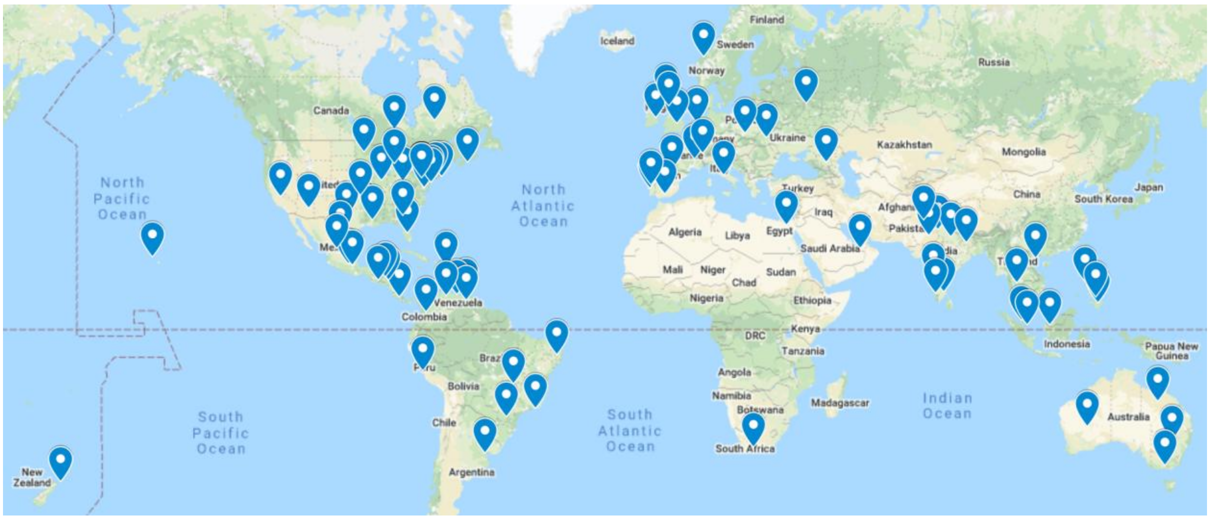
Table 2-10 Technology Tools for Recruitment

Technology Tools/Methods	**Definition**	**Data Collection**
ZOOM	online synchronous video communication	Confirmatory Interview
Telegram	encrypted instant messenger	Survey
Email	use technology to communicate over the Internet	Survey Distribution, Recruitment
phpBB Discussion Board	website used for discussion on a specific topic	Focus Group
Google Forms	survey application used to create a distribute forms	Surveys
YouTube Videos	create and upload videos (private or public)	Welcome and Overview
Social Media: LinkedIn, Twitter, Instagram, Reddit,	online communication for social networking	Recruitment

There are several well-documented advantages to online data collection (Hamilton & Bowers, 2006). For this particular research, the advantages worked heavily in favor for the technical nature of our questions and respondents' abilities (Table 2-10 Technology Tools for Recruitment) and (Lefever et al., 2007). Some of the positive aspects of remote communication and data collection are referenced in Figure 2-5 Map of all Data Collection Participant Locations:

- Increased Standards for Selection
- Increased Population for Selection
- Location Independence
- Time Zones/ International sampling
- Convenience (without Convenience Sampling Methods)
- Document Exchange
- Automated Transcription
- Thoughtful Responses
- Extra Time to Prepare

Figure 2-5 Map of all Data Collection Participant Locations



Note. Map created with Google Maps data 2020

An online discussion group and online surveys also provided participants time to ponder and think about their responses instead of being put on the spot in one meeting. It also allowed me time to think about their responses and prepare appropriate follow-up questions (Hamilton & Bowers, 2006). A full list of the question types used for this research is displayed in (Table 2-11 Data Collection Question Types). A disadvantage of remote data collection was the absence of non-verbal cues when not in a video conference, or, when the video conference was even slightly low quality. This was an unfortunate reality for some video calls; however, it did not seem to impact the respondents' contributions to the study. This could also be seen as a personal perception that was not shared by the affected respondent.

Table 2-11 Data Collection Question Types

Data Collection Method	**Question Type**			
	Multiple Choice (one answer)	**Drop Down**	**Open-Ended**	**Matrix (multiple answers)**
Expert Interview: Part 1	yes	--	yes	yes
Expert Interview: Part 2	yes	--	yes	yes
Confirmatory Individual Interviews	--	--	yes	--
Focus Group	--	--	yes	--
Job Functions Survey	yes	--	yes	--
Cybersecurity Interest-to-Function Survey	yes	yes	yes	yes
Cybersecurity Interest-to-Function Online Questionnaire Final Survey	yes	--	--	yes

2.5 Data Analysis for the Artifact Build and Evaluation Phases

2.5.1 Coding

The secondary data was subjected to codification to expose repetitive and unique identifiers for both individual interests and cybersecurity functions (Bhattacherjee, 2012). This was primarily performed through the use of the UNIX and Linux tools: cat, grep, sed, awk, sort, uniq, head, tail, rev, cut, printf, echo, and reductive for loops. The Internal Field Separator (IFS) was modified to provide for consistent and coherent data output where carriage return, newline, or blank-space was not sufficient for proper analysis. Minor work was performed through Gnumeric to ensure a clean representation of the data (Saldaña, 2015).

2.5.2 Thematic Analysis

After the initial codification, thematic analysis was performed to find the underlying meanings of the interests and functions (Clarke & Braun, 2017; Guest et al., 2012). This required all of the identified interests and cybersecurity functions to be narrowed based on meaning, rather than explicit terminology. This was also true for variations in English between functions and interests as taken from an international context. This required the repetitive processing of the lists to provide a final outcome.

2.5.3 Descriptive Statistics

The initial survey data was subjected to descriptive statistics to provide a basic summation of the collected information for analysis. This was valuable in the initial review of the data to ensure that means were achieved from several locations for each of the interests and functions identified. This was also valuable in the interest-to-function alignment survey to present the most pertinent traits or tasks for each interest or function, respectively.

2.5.4 Visualization

Beyond descriptive statistics, UCINET and NetDraw were used to visualize the relationship between each of the data points for both interests and functions. Link-Analysis or Social Network Analysis techniques allow for the immediate identification of positive or inverse correlation of a data set (Boddy et al., 2017). Regarding individual interests, an inverse correlation was evident between each of the descriptors. This indicated that there was minimal ambiguity between the traits selected. In regard to the cybersecurity functions, a positive correlation indicated that each of the functions did relate to cybersecurity. This technique could be further exploited to provide nested groups of the information to reveal additional insights into the alignment of interests-to-functions.

2.6 Ethical considerations

As this research analyzed the results for individuals in a subset of the population, it did not require any personally identifiable information to be collected. Careful consideration was taken to minimize any ethical concerns regarding this research. The initial design of the questionnaire avoided specific questions about an employee's desire to maintain employment at their specific employer and refers to general traits of work that are of minimal ethical impact in the event of public disclosure. If the questionnaire answers were publicly disclosed, the system did not collect any personally identifiable information, nor could the individual's Internet address be tracked. The system provides complete anonymity, avoiding common ethical concerns regarding personal information loss or disclosure.

There is a slight probability that an individual's employer would provide video recording of the employee's desktop or full interception of any traffic transmitted from an employee's workstation. In such a case, the survey will provide a statement, "If there is any concern that this survey would violate your organization's policies, or that your employer may interpret any comments recorded in this survey in a negative fashion, we request that you perform this short survey at another time and location. Your time and assistance is greatly appreciated."

The informed consent, non-disclosure agreement, and permission letters were required before any data collection began to meet compliance with the ethical considerations for this research (see Appendix B.1 Informed Consent, B.2 Non-Disclosure Agreement (NDA), and B.3 Company Permission Letter). Every effort has been taken to consider ethical assurances for each participant during the entire data collection process, including the anonymous nature of all participants.

Informed Consent

The informed consent was required for all participants in this research (see Appendix B.1 Informed Consent). It clearly describes the project information for this research study by providing a brief description of the research, research objectives, and that there are no perceived risks. The last section of the informed consent states the following:

- I hereby voluntarily grant my permission for participation in the project as explained to me by Paul W. Poteete.
- I understand that my data will be kept anonymous.
- I understand the Research Study Description and the Research Study Objective as described above.
- I understand that participation in this research is voluntary, and it is my right to choose whether or not to participate in this research.
- I understand that the information furnished will be handled confidentially.
- I understand the nature, objective, and any possible health implications of this research.
- I understand that the results of the survey may be used for the purposes of publication.
- I understand that I may print this consent form if I would like to retain a copy for myself.

All of the respondents participating in this research through the online survey, focus groups, and interviews must agree to the consent document. The Informed Consent specifically states: “I understand that participation in this research is voluntary, and it is my right to choose whether to participate in this research.”

The following are example statements to which the participants agreed before participating in this research: "I agree with the anonymous nature of the Informed Consent." Or "I accept the Informed Consent Requirement."

Non-Disclosure Agreement (NDA)

The NDA was required for all interviews, focus groups, and surveys (see Appendix B.2 Non-Disclosure Agreement (NDA)) The NDA describes the research objective and overview. All participants must accept and agree to the NDA before participation is allowed. The last section of this form states the following:

Participation in this research constitutes acceptance of the statements below:

- Any concepts discussed by other participants, whether technical, personal, or business-related, will be held in strict confidence. I will not take advantage, either for profit or reputation, of any information disclosed within this meeting.
- Any ideas, inventions, devices, or developments, that are patentable, publishable, or worthy of personal or professional gain will be the property of the originating individual, except where it specifically pertains to the CyberBridge Research.
- I will not disclose any Personally Identifiable Information (PII) concerning the other participants in this meeting.
- No notes that contain any sensitive information are to be removed from this meeting, except where those notes directly relate to CyberBridge research.
- All CyberBridge research notes will be open to inspection and approval by all parties involved.
- All participants will receive a digital copy of this form.

The utmost care and concern has been taken to ensure the research participants' opinions in this research will be anonymous and kept in strict confidence. The following excerpt is an example from the various data collection methods, showing that the participants were required to read and accept the informed consent and NDA before participating in this study. “Do you agree with the Anonymous nature of the Informed Consent and Non-Disclosure of any information that may be somehow shared during this survey?”

The informed consent and NDA were made clear in communications before data collection began. The following example is an excerpt from and email I sent to potential focus group participants: “The results are entirely anonymous; however, I must collect your name and organization name to comply with international ethics validation. Again, neither your name, your organization's name, nor your email will be listed in the final document or any associated research."

Permission Letters

An organizational approval letter was required for participants for a portion of the data collection processes in order to protect the companies from any liability or disapproval (see Appendix B.3 Company Permission Letter). The purpose of this form is clearly stated in the letter: "In order to ensure ethical procedures in data collection, this form is presented to this organization as a request for private discussions with individuals who may work in your organization."

2.7 Summary

This research used several data collection and documentation analysis methods across several sources to understand the problem, and design, build, and evaluate the artifacts as a solution. This followed a pragmatic mixed-methods approach within the design science research methodology. Due to the content of the research, an emic epistemology was necessarily assumed within the content and research topics along with empirical methods. This study further identifies ontological viewpoints in pragmatic systems as the composition, collection of entities, the inter-relatedness of the entities, and the hierarchy of those entities in reality, and, relative to themselves.

3 Literature Review - Problem Awareness

In designing a cybersecurity interest-to-function career alignment model, this research investigated existing solutions for career-interest alignment and models (Jackson et al., 1984; Liao et al., 2008; Wille et al., 2010). This soon developed into a search to determine the functions within cybersecurity roles and which of those functions would be of use. As the goal of this research concerns the relationship between an individual's interests and cybersecurity functions, additional research was conducted into what interests would be of use in analyzing a relationship to purely cybersecurity functions. This investigation resulted in two main directions in literary review: well-established academic literature and professional literature. Although there were several psychometric analyses and interest-based approaches in academic literature that provided insight into individual predilection for certain job functions and various management structures, it soon became evident that there was a paucity of resources within the formal academic literature for cybersecurity functions and their relationship to interests (Dreibelbis et al., 2018; Newhouse et al., 2017). Furthermore, it became apparent that within the professional literature and employment databases that described cybersecurity job titles and functions, that there was not a consensus on what constituted cybersecurity-centric job functions (De Haes & Van Grembergen, 2004; Lewis & Rivkin, 2000; Newhouse et al., 2017; Security Wizardry, 2018). It is true that many functions are shared among several different career roles; however, this is not in exclusion to the existence of particular functions that are specific to cybersecurity roles. The inadequacy of existing literature for cybersecurity roles and functions, outside of the alignment to individual interests, generated additional awareness of the scope of this problem. The research would need to first identify and categorize cybersecurity functions from several sources before any consideration of which interests might be relevant to those functions could be determined, and finally, how those functions and interests should be aligned.

3.1 Specifying Cybersecurity Functions (Artifact 01 / Proposition 01)

There are thousands of current cybersecurity titles and related job descriptions reported online (Zeltser & Hoyt, 2015). The complexity of the cybersecurity field is similar to what is seen in the healthcare industry, but far fewer people are familiar with cybersecurity functional distinctions (Meeusen et al., 2010). Cybersecurity functional identification is further complicated by the plethora of cybersecurity job titles that are utilized to describe similar or identical roles in an organization. Often, the cybersecurity tasks overlap, masking the true meaning of the individual's role. Additional research was required to determine what and how a function would be ascribed to a cybersecurity role (Table 3-1 Key Theories and Concepts for Job Functions: Proposition 01.

Table 3-1 Key Theories and Concepts for Job Functions: Proposition 01

Theory	Key Concepts	Relevant Aspects of Theory
Role Conflict and Role Ambiguity **(Johnson 1975, Rizzo 1970)**	• Tasks within roles may be contradictory or ambiguous.	• Defining cybersecurity functions within roles can be complicated by contradictory or ambiguous requirements.
Role Theory **(Katz and Kahn, 1978; Biddle, 1986)**	• Work role requirements • Work role behaviors • Occupational groupings • Job function	• Members assume different roles associated with the particular jobs they are hired to perform in order to complete various tasks.
Taxonomy Development in Information Systems **(Nickerson 2009, 2010)**	• Taxonomy • Development of Taxonomy	• Classifying objects of interest into a taxonomy.

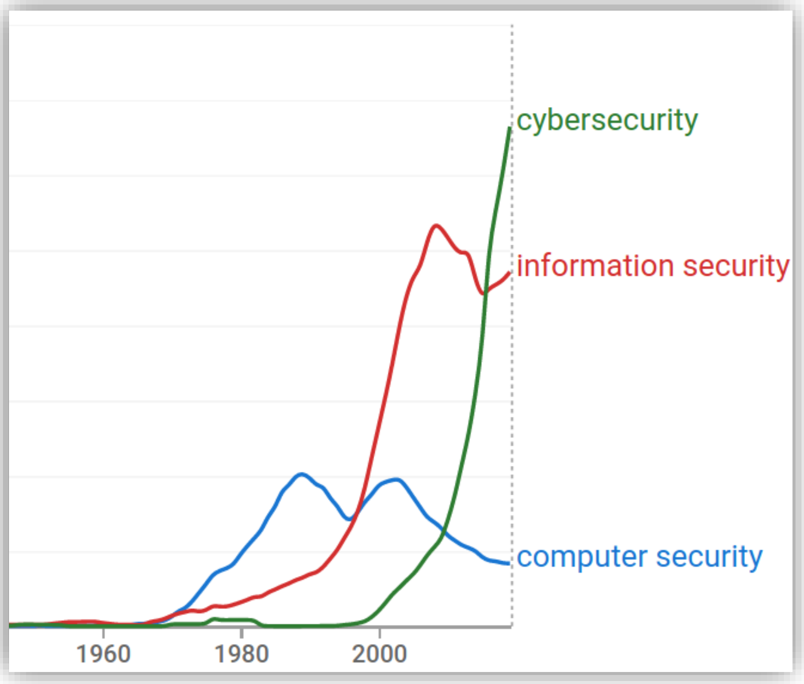
Note. The key concepts and relevant aspects of the three theories used to develop Proposition 01 and Artifact 01 are provided for a brief overview and reference as well as a foundation for the development of the cybersecurity career job functions.

3.1.1 The Problem of Classifying Cybersecurity Functions in Academic Literature

Initially, the problem seemed to be easily defined into concepts of classification, functions, and cybersecurity; however, it was soon determined that even what seemed to be the simplest concept of classification was riddled with ambiguity (Nickerson et al., 2010). It was determined that research into classification or categorization from a general perspective would not be as useful for this specific topic of research; as such, cybersecurity concepts were persistently applied to any review of taxonomy or classification (Newhouse et al., 2017). This complexity may also been seen in Morgeson & Campion's definition that a work role or function may be seen from the perspective of both tasks performed by the employee or also their capabilities, preferences, and opinions (Morgeson & Campion, 2000). This extends a function beyond what is easily perceived through observation of activities into the unknown or imperceptible reasoning that is involved in the employee's selection of a particular method or action. This opens new facets of function to include the activity, the objects involved in the activity, and the purpose or response of the activity (Fine & Getkate, 1995). In Role Theory, tasks are interpreted through the lens of employee role behaviors, and these work requirements can involve specific tasks to general responsibilities (Katz & Kahn, 1978). This ambiguity of terms and semantic discourse can be seen throughout foundational theories, concepts, and definitions, possibly due to the interwoven nature of the English vocabulary in which the theories were written. Semantics accounted for, Katz and Kahn's concept of role expectations may explain why some individuals perform functions in similar fashion (Katz & Kahn, 1978). Tasks are then considered to be a part of a function or role, if the function is synonymous with the term role. If function is seen as synonymous with the task, then an employee's role or title becomes a less descriptive, higher-order, categorization (Lewis & Rivkin, 2000). This research evaluated the titles and roles to produce a list of tasks or functions performed by employees. To simplify this concept, this research follows the traditional hierarchical order of role and title as representative of higher-level descriptions within which are found specific tasks and functions. Again, this hierarchical role and title to function and task categorization is not consistent within research literature but is defined here to allow for disambiguation when viewed within other literary sources. Furthermore, the reader must be careful to dynamically adjust the semantic meaning for each of these classifications, as tasks and functions, as well as roles and titles, have been shown to influence job satisfaction, performance, and retention motivation (Biddle, 1986). The problem of classifying cybersecurity functions continues to extend beyond the complexity experienced in many other fields due, in part, to the technical nature of working within systems of systems (Dodge et al., 2012; Holtom et al., 2008). As cybersecurity overlaps with other technical fields, further delineation was performed for security-centric aspects. This added to the fundamental challenge in all sciences of classifying roles and function theories (Biddle, 1986). When taking into consideration the multitude and depth of functions in a technical or cybersecurity position, the act of defining cybersecurity roles and functions was daunting. Beyond the delineation of functions, the creation of a taxonomy from those functions needed to be established. Creating taxonomies has been forever plagued with difficulty across industry and science (Nickerson et al., 2009). This combination of functional role determination and the respective categorization of those functions presented a daunting challenge. This research provided definition and categorization to allow for a better understanding of cybersecurity functions.

Another issue that arose was the potential misunderstanding of what cybersecurity would actually represent respective to each task or function within each classification (Nickerson et al., 2009, 2010; Ulum, 2018). In order to properly classify cybersecurity functions, one must first define the meaning of the terms, cybersecurity and function (R. Von Solms & Van Niekerk, 2013). To better understand this relationship, a short background of how its developmental history is framed within this research could be of assistance. The immediate origins of cybersecurity come from the early concepts of computer security, and later, information security. The relationship of this terminology may be seen in the Google NGram. (see Figure 3-1. Cybersecurity Terminology Increase) (Lin et al., 2012).

Figure 3-1 Cybersecurity Terminology Increase



Note. Screenshot created using the tool from Google Ngram site, https://books/google.com/ngrams (Lin et al., 2012)

The original term that is mostly closely aligned to today's information security would be the expansion of computer Literature Review Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions security from the 1960s. Computer security became commonly referenced as information security in the 1970s and beyond (Lin et al., 2012). The need to define cybersecurity versus information security was based on those forms of misunderstanding, as well as other notable complications that arise from a misinterpretation in the past and present (R. Von Solms & Van Niekerk, 2013). In this research, cybersecurity was seen as the symbiotic relationship between autonomous and manually controlled security systems. This was based on earlier concepts of cybernetics (Wiener, 1948/2019). Providing greater specificity for the term cybersecurity allowed us to define this symbiosis beyond limited concepts of information or computer security that may instead represent a system entirely driven by human intention. In this case, a cybersecurity system was composed of both autonomous and manually configured aspects, understanding that systems may operate beyond predefined patterns and exhibit a form of artificial intelligence that worked in concert with human operators. The concept that cybersecurity was more than a system controlled entirely through human policy, but a system whose autonomy was facilitated through the direction and control of human intention may further complicate the understanding of cybersecurity functions (Colwill, 2009; Colwill & Jones, 2007; McClain et al., 2015; Mikolic-Torreira et al., 2016). The orchestration of that autonomy as combined with human intention and learning became a foundational aspect of cybersecurity tasks. To provide a bit of clarification, cybersecurity was seen as an actual cooperative effort between both machines and humans, and this cooperation must be understood as part of the functional delineation from roles.

Another concept of cybersecurity was concerned with the notion of security in a technical, physical, or administrative sense (Said et al., 2014). In this, the challenges surrounding cybersecurity functional and organizational alignment were seen as extending into a form of asymmetric battlefield operations that were conducted invisibly alongside normative organizational processes (Martini & Choo, 2014). The difficulty of implementing cybersecurity programs was interpreted as a combination of a lack of understanding of cybersecurity functions, the proper individual alignment with those functions, and how those functions may be communicated in business terminology. Organizational operations, including technical operations, can be measured against well-established productivity models (Park & Shaw, 2013). This may be contrasted with cybersecurity threat models that are being actively developed in such ways that organizational policies, standards, and procedures may not be able to maintain the magnitude of changes that occur from one day to the next (Mikolic-Torreira et al., 2016). This concept was a militaristic viewpoint of attack and defense, noting objects that are protected as well as those that present threats. It may be completely devoid of any understanding of the synergistic orchestration of human and machine, but simply denoted the existence of threats and defensive measures. In this case, cybersecurity involved the prevention, detection, response, and deterrence of malicious or detrimental events. Conceptually, the two meanings of cybersecurity have been separated in this research as a definition that operates within the operational aspects of the subject versus the adjectival or descriptive term used to define the broad individual function. Although the adjectival or subjective use of the term may be defined from slightly different viewpoints, this research viewed cybersecurity from an integrated viewpoint. The concepts around threats and defenses worked into our understanding of the symbiotic relationship between machines and humans (Ramirez & Choucri, 2016). This holistic viewpoint presented cybersecurity controls as the foundation of employee functions as composed of all of its requirements and the orchestration of efforts to provide protection to an organization, a person, a process, or other technology.

Several theories that discussed role and function from an individual and organizational standpoint were evaluated, but found to be either too broad, or unrelated to cybersecurity functions (Biddle, 1986; Joseph et al., 2007, 2012; Katz & Kahn, 1978; Nickerson et al., 2009, 2010). In most cases, theories examined an organization's need or an individual's extrinsic motivations to maintain employment. This research also avoids the specific issues surrounding competence, competency, and training. In this case, individuals are understood as being technical competent for their position, allowing the analysis to be based on their interests and not their abilities. Although discussions in competence and competency are entirely valid when discussing technical or complex positions, it is out of scope for this particular project (Bassellier & Benbasat, 2004). The former theories are entirely valid in their proposals, but they are inadequate in their appreciation for the specific functions encountered within a cybersecurity role. In cases where daily activities were interpreted, the individual's preferences were based on a seemingly universal appreciation or rejection of a particular task (Heavey et al., 2013). This research examined the individual motivations based on interests that were related to specific categories of cybersecurity functions. In this way, no task was seen as monolithic. In this, no task was seen as being universally enjoyable or unpleasant for all individuals. Some individuals may enjoy tasks that others find unpleasant. Additional theoretical foundations were found that examined individual industries, such as healthcare. In those cases, functions were not delineated or categorized in such a way as to provide a model or solution but were reviewed on qualitative research methods (Meeusen et al., 2010). Beyond these cases, other research has been conducted on the employee's desire to maintain or terminate employment based on intrinsic or extrinsic factors; however, none of the discovered theories defined individual interests to cybersecurity functions. Role Theory was examined as a potential solution to categorize employee functional constructs (Biddle, 1986; Katz & Kahn, 1978).

Even though role conflict and role ambiguity are comprehensive concepts for the understanding of job functions and roles, they do little to inform the tasks and functions within cybersecurity (Johnson & Stinson, 1975). Although it is very true that roles will have several functions, often in conflict with one another, this does little to inform the specific circumstances surrounding the description of cybersecurity tasks and functions. This is also true for role ambiguity, as there are certainly occasions where a function or task is poorly defined, especially within the cybersecurity discipline; however, this does not assist with the creation of a comprehensive or categorical listing of functions, nor does it provide a process by which this methodology may be defined (Rizzo et al., 1970). This research seeks to explore the tasks or activities that the role holder within cybersecurity needs to perform. Despite a plethora of resources involving role, function, retention, and organizational hierarchy, there is little research on the specific functions experienced within the cybersecurity profession in academic literature. Understanding cybersecurity functions is critical for interest-to-function alignment models. There are several models for general employment as well as technology employment for alignment; however, cybersecurity positions are aligned in a monolithic view, missing the distinctions that are so critical to understanding functional variation. As the goal of this research requires the original delineation of cybersecurity functions, it is deemed appropriate to explore the professional literature for additional insight. In this case, the importance of title or roles may be minimized in deference to the actual tasks or functions performed by the cybersecurity professional.

3.1.2 Challenges and Advancements in Cybersecurity Professional Organizations

The concepts related to cybersecurity roles may be largely misunderstood within industry as a result of the immaturity, novelty, and complexity of their functions. The challenge of defining the complex functions within these roles is exacerbated by the unique novelty of many of the new capabilities and threats. Also, as many of these roles have only existed for three to ten years, individuals who work within the respective industries, and who provide related functions, are often capable of providing insight into their actual function. In order to provide this additional insight into cybersecurity functions, several professional frameworks, organizations, employment databases, and academic work on professional governance models were examined. Through this examination, categories began to become better defined operational, defensive, and offensive. The operational functions are those tasks that may be scheduled, are procedural, and may be seen as routine from an organizational or cybersecurity standpoint. The defensive functions contain more dynamic tasks that require planning and design heavily reliant on the ever-changing vulnerabilities, exposures, threats, and political structure of the organization. The offensive functions emerged as containing those tasks that are necessary in attack or penetration testing, such as against an opponent, for research, or to determine security an organization's security preparedness. The operational functions are better defined and understood, as they may be more easily written as procedures, conducted over several decades, especially since the advent of large-scale use of computerized resources from the 1970s. This creates a rapid pace of development of not only new technologies and their associated risks, but of these particular employee functions within roles surrounding those technologies (DeSilver, 2014). The ambiguity of cybersecurity operational through offensive functions may be seen in a study that researched 348,975 cybersecurity-related jobs, found that the top technical skills that are in demand are as follows: Information Security, Network Security, Linux, Information Systems, Cryptography, Cisco, and Technical support/customer service (Workforce Intelligence Network (WIN), 2017). This is further illustrated through the high rates of turnover regarding technical jobs around the world (Caldwell, 2013). It is important for organizations to understand the organizational needs for cybersecurity, as well as the functions within cybersecurity title or roles. Although this research reassesses the functions within the roles, it is necessary to understand the roles and how they imply function. As a foundation for role and function usage within an organization, information technology and cybersecurity governance literature were reviewed. These self-governance and external governance initiatives were created to fill the need to manage the largely unregulated use of technical and cybersecurity skills and technology within the local and global market systems (De Haes & Van Grembergen, 2004). Governance organizations had provided business alignment resources for technical departments for a number of years, allowing for clear objectives to be defined. This additional clarity provided for better alignment and productivity within the organization and the IT department (Weill & Ross, 2005). Although many organizations many not have a governance model that would allow for clear alignment of their business objectives to cybersecurity operations, the usage of governance models provides, at the very least, a checklist of activities that render a positive outcome for almost every organization (Ping-Ju Wu et al., 2015; B. Von Solms, 2005).

Cybersecurity frameworks provide organizations with structural and procedural support for organizations to assist in the development of thorough cybersecurity strategies. Within the cybersecurity industry, frameworks are defined by for-profit, government, or non-profit consulting or counseling organizations to provide guidelines for how an organization should secure their assets (De Haes & Van Grembergen, 2004; International Information System Security Certification Consortium (ISC)^2, 2018; ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2014; Lewis & Rivkin, 2000; Newhouse et al., 2017; *SANS Inst.*, 1989). These frameworks may define cybersecurity titles, functions, organizational hierarchies, policies, physical design considerations, technical component purchase recommendations, and more. This may be in contrast to some academic literature that seeks to provide a more holistic solution over specificity of structure; however, the frameworks are designed to provide less of a theoretical solution and more of a practical solution. As is true with many practical applications in the absence of proper theory, they become overly specific, resulting in frequent misalignment or rigidity. This is not intended to criticize the inadequacy of the frameworks for professional application; it is simply stating that the frameworks provide guidance of how to conform to their specific guidelines, not on what authority those specific guidelines where originally created.

A small portion of leading frameworks is dedicated to advancing the concepts of cybersecurity roles within organizations (Greene, 2014). These explanations are often ambiguous or contradictory, as in the definition and purpose of a cybersecurity analyst, or conversely, they may have reached considerable consensus, as in the description of the duties of a Chief

Information Security Officer (CISO). Although the functional tasks associated with each respective cybersecurity role may be a small portion of the framework, an understanding of the ultimate goal of each respective framework allows deduction into what individual responsibilities may be required for distinct organizations (Alexander & Cummings, 2016). In some instances, frameworks establish educational requirements and categories for cybersecurity roles without the need for specific title designations. This may allow an organization to address the most fundamental needs of the program without the complications found in politicized role titles (Newhouse et al., 2017). In the course of framework selection, an organization should strive to align the framework with their regulatory and industrial needs, as well as their cultural foundations. The two frameworks discussed in this portion of research are the National Institute for Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) and the International Organization for Standardization (ISO). The types of frameworks and organizations discussed are provided in Table 3-2 Types of Frameworks and Organizations. Although this is not a comprehensive list, it does provide a representative expression of interests (Greene, 2014; Newhouse et al., 2017).

Table 3-2 Types of Frameworks and Organizations

Types of Frameworks	Examples
Formal Frameworks	• **NIST / NICE** National Institute for Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) (Newhouse et al., 2017) • **The ISO27000 Series** International Organization for Standardization (ISO) (ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2014)
Professional Organizations	• **(ISC)² ®** International Information Systems Security Certification Consortium (International Information System Security Certification Consortium (ISC)^2, 2019) • **ISACA** ® Information Systems Audit and Control Association (Otero, 2018)

Types of Frameworks	Examples
Training Organizations	• **The SANS Institute** SysAdmin, Audit, Network and Security (SANS) Institute (Paller, 2020) • **InfoSec Institute** Information Security (InfoSec) Institute (InfoSec Institute, 2020)
Occupational Databases	• **The O*NET Program** (Lewis & Rivkin, 2000)

The cybersecurity industry is largely unregulated. This lack of regulatory authority may stem of a lack of understanding, the obscure or illegal nature of much of its content, the lack of agility of bureaucratic organizations to radically change foundation and direction to create meaningful policies, or all of these factors and more (Disterer, 2013). This creates opportunity for professional certification and training organizations to fill the gap where legislation dare not tread. Professional cybersecurity certifications establish a set of requirements for their patrons, that when achieved, the patron may claim mastery over a specific or general cybersecurity field of knowledge and display a credential. Due to a lack of ability or a lack of desire for organizations to properly assess the cybersecurity knowledge of their staff or candidates, they must rely on certifications for guidance. This has led professional organizations to possess substantial influence in the training and promulgation of an assorted collection of cybersecurity careers. One such certification, the Certified Information Systems Security Professional (CISSP®), provided by the International Information Systems Security Certification Consortium (ISC)^{2}® is internationally respected as a significant certification for senior cybersecurity professionals (International Information System Security Certification Consortium (ISC)^{2}, 2018). This certification is currently accepted within many national governments as proof of knowledge as part of their cybersecurity professional requirements. Next, the Information Systems Audit and Control Association (ISACA®), has international distinction for their certifications, the Certified Information Systems Auditor (CISA®) and the Certified Information Security Manager (CISM®) (Information Systems Audit and Control Association (ISACA), 2018) . Although there are many professional organizations offering several certifications, (ISC)^{2}® and ISACA® are highly regarded and representative of certifications within the security industry as providing authoritative training and education.

Many of the certifying bodies have also introduced their own training materials and organizations that have advanced into the educational system and now provide authentic degrees in cybersecurity; however, most are content to provide guidance and training for their professional brand of cybersecurity credentialed certifications. In both the academic and vocational training cases, these organizations provide criteria from which individual skill may be assessed. To address the complexity of preparing individuals for cybersecurity functions, several organizations have arisen to train individuals interested in cybersecurity for their future careers. Two representative institutions are: the SysAdmin, Audit, Network and Security (SANS) Institute, and the InfoSec Institute. These organizations provide specific training for tasks encountered in everyday work by cybersecurity professionals. SANS is a large provider of cybersecurity training, leading individual training in defensive and forensic capabilities (*SANS Inst.*, 1989). The InfoSec Institute is a newer organization that gained popularity through the introduction of an ethical hacking certification. As InfoSec Institute has grown, it has become internationally recognized for its hands-on, practical training (Infosec Institute, 2018). Both of these organizations represent a multitude of training organizations that are now dedicated to cybersecurity career training. This allows occupational databases that contain job statistics and functional definitions of vocational tasks to align certifications or skills with metrics for technical career selection. The O*NET Program provides validated data for the entire United States workforce which is freely available for scientific or personal research purposes (Lewis & Rivkin, 2000). The constant updates from millions of accounts every year provides a wealth of information regarding careers. The incorporation of various alignment metrics within the career database provides insight into potential interests-to-function alignment for many careers. This allows for extensive data to be drawn for general careers that could possibly be related to cybersecurity career performance and satisfaction.

Although this research is not concerned with the regulatory or specific certifications provided by any entity, the content acquired from these resources is useful in defining cybersecurity titles and roles, and, tasks and functions, as these organizations have dedicated resources to identifying challenges and opportunities for cybersecurity staffing. Although several advancements in understanding cybersecurity topics, controls, and functions have been made through the research and popularity of these organizations, they are designed around their own viewpoint of cybersecurity functions and organizational needs (Campbell et al., 2015). Understanding that their viewpoints are self-serving, researchers may compare and contrast the professional organization's relevant recommendations surrounding the thousands of cybersecurity topics and use the information for future theory development. As organizational certification requirements and training guidelines become more refined, the clarity of each function required within cybersecurity roles becomes more defined. This current level, and increasing levels, of clarity surrounding each position allows this research to more accurately define the alignment of cybersecurity functions to individual interests, especially in regard to performance, satisfaction, and potentially retention. This may be seen in the NICE framework's expression of career development, training requirements, human resources development planning, or descriptions in (Newhouse et al., 2017).

3.1.3 Proposition 01: Taxonomy of Job Functions

The goal of this study is to help cybersecurity professionals and organizations better understand cybersecurity careers and how individuals align to the functions therein. The job function of a cybersecurity professional describes their daily tasks completed while at work and must be initially understood before any model of alignment to individual interests and organizational needs can be constructed. Through an examination of well-developed academic literature, it was determined that there exists a lack of formal academic research into the categorization of cybersecurity titles and functions. This required the incorporation of professional frameworks, training organizations, and career databases as contributors to the development of this research. The academic resources provided grounded principals and theories for general employee motivation and organizational performance. These general concepts were augmented in some cases to include technical employment theory that could be seen as incorporating tangentially related concepts of cybersecurity roles and functions, in the most general sense. Although the academic literature was limited, it was useful in the conceptual formation of a new model; although, it was inadequate in modeling cybersecurity functions themselves. Where the academic literature was deficient, the professional resources were prolific in their inclusion of roles and functions according to their respective viewpoints. None of the literature reviewed would provide alignment of individual interests to cybersecurity functions. In cases where functions were referenced, there was no consensus of function. This research provides a categorization of cybersecurity functions for use in a new model that will align these functions to individual interests. There was little discussion in the academic or vocational literature that would answer what functions would be of use, how to categorize those functions, or even consensus on what would be included in a library of functions.

Proposition 01: Taxonomy of Job Functions

Therefore, this research proposes the development of a taxonomy of cybersecurity functions for use in a new model that will align to individual interests.

3.2 Specifying Individual Interests within Cybersecurity (Artifact 02 / Proposition 02)

In order to associate individual interests to functions within cybersecurity roles, concepts for functions and interests must be properly defined. This includes an examination of the assumption that personality traits play a factor in job satisfaction, performance, and retention (Aruna & Anitha, 2015; Holtom et al., 2008; WeiBo et al., 2010). In the prior section, cybersecurity functions are established. In this section, individual interests that relate to cybersecurity are identified. This process presents a number of questions, mainly those that investigate ways to define and measure individual interests, as well as, what individual interests would be applicable within the cybersecurity profession. In this research, an individual's interests go beyond their personal psychology to the applied factors that provide intrinsic motivation (Oudeyer & Kaplan, 2007; Ryan & Deci, 2000). This new interest inventory must be broad enough to allow for generality in categorization, while sufficiently pointed to be of use in establishing explanations of individual desire and behavior within cybersecurity. In general, this dichotomy is a common challenge within taxonomy development and industry initiatives for retention studies; however, the inclination to describe interests as they apply to retention or general performance for roles outside of cybersecurity requires caution to avoid inappropriate correlation (Gati et al., 1996; Jackson et al., 1984; Nickerson et al., 2010). As such, this amalgamation of interest to purpose is useful, but differentiated to allow respective purposes outside of those within the cybersecurity profession to be excluded based on the functions in section 3.1. This allowed psychometric concepts, vocational interest studies, and career interest libraries to be aggregated and categorized into a small subset of interests that were relevant to cybersecurity professionals. It is important to note that in cases where cybersecurity was referenced, cybersecurity was seen as a monolithic occupation with a lack of diversity of function. In those cases, the role, "cybersecurity professional" was seen as equivalent to a personality trait (Ogbanufe & Spears, 2019). This research looks more deeply into cybersecurity roles to differentiate tasks and functions, and why some individuals may prefer particular tasks over other tasks Table 3-3 Key Theories and Concepts for Job Interests: Proposition 02.

Table 3-3 Key Theories and Concepts for Job Interests: Proposition 02

Theory	Key Concepts	Relevant Aspects of Theory
Agency Theory **(Mitnick, B. M., 1976)** **(Jensen & Meckling, 1976)**	• Egoism • Self-interest	• Leadership and shareholders are imbalanced and egotistical is possibly an oversimplification in study.
Five Factor Model (FFM) **(Digman, 1990)**	• Adjectives / Traits • Groups personality types into five factors or traits	• Model is a more general tool to provide initial personality evaluations. • Model is similar to the way cybersecurity-related interests may be codified.
Gati's Model **(Gati, 1996)**	• Method to create a taxonomy of career decision difficulties	• Creation of a survey. • Creation of a taxonomy.
Holland Vocational Interest Inventory (RIASEC) **(Holland, 1986)**	• Careers • Psychometric testing	• Provides the most specific analysis of the psychometric analyses. • Careers correspond to the RIASEC scores.
Job Characteristics Model **(Hackman & Oldham, 1976)**	• Job performance and satisfaction • Personality traits related to employee satisfaction	• Foundation for subjective identification of personality traits as influential to career output.
Jung Typology **(Jung, 1921)**	• Relationships and personalities	• Extroversion and introversion on a scale best-suited for a general identification of adaptation to what seems to be a procedural focus, not a specific task or function.
Met Expectations **(Porter and Steers, 1973)**	• Employee interests and expectations	• Individual concepts of expectation as a significant factor of satisfaction and retention.
Self-Determination **(Deci and Ryan, 2008)**	• Motivation based on intrinsic and extrinsic factors • Individual competence, autonomy, and relatedness	• Provides a basis for motivation as a part of personality.
Taxonomy of Vocational Interests **(Jackson et al, 1984)**	• Individual personality factors • Interests and themes • Career field association	• Classification and alignment of individual personality traits to functions.
Unfolding Model **(Lee and Mitchell, 1994)**	• Psychological paths that people take when quitting • Why and how people quit	• Individual personality is not thoroughly investigated. • Research was retention-centric, and satisfaction played a key role.
Withdrawal Model **(Hulin 1991)**	• Withdrawal behaviors • Job Satisfaction	• Behavioral modeling involves individual inclinations and profiling.

Note. The key concepts and relevant aspects of the eleven theories used to develop Proposition 02 and Artifact 02 are provided for a brief overview and reference as well as a foundation for the development of the individual interests.

3.2.1 The Problem of Classifying Cybersecurity Interests in Academic Literature

The challenges surrounding the classification and categorization of interests, as they apply to the cybersecurity field, were approached in several different models in the past (Kaufman et al., 2013; Nickerson et al., 2009). Given, none of the models specifically addressed cybersecurity professionals; however, they illuminated the challenges with the classification and categorization of interests for a profession. Initially, individual personality was not considered a factor in career satisfaction or performance, as all individuals were considered to be part of a somewhat collective mindset, as represented in the Self-Determination or Agency Theory (Deci & Ryan, 2008). The conceptual deficit regarding individual interest to career function possibly continued until the advent of Jackson's Taxonomy of Vocational Interests (Jackson et al., 1984). This is complicated by the obscurity and dearth of cybersecurity personality traits, as well as, the complicated process of creating a taxonomy of any kind. In general, the Self-Determination (Deci & Ryan, 2008), Agency (Mitnick, 1976), and Met Expectations (Porter & Steers, 1973) theories employed collective interpretations of employee interests, while the Unfolding Model (Lee & Mitchell, 1994) and Jackson's Taxonomy of Vocational Interests (Jackson et al., 1984) began research into individual personality factors (Hom et al., 2017). In all of the cases examined, there was an insufficient amount of research dedicated to the cybersecurity profession and interests that would specifically apply to cybersecurity professionals.

To begin the journey of collective to individual personality and interest, the author of the Self-Determination Theory provides a basis for motivation as a part of personality (Deci & Ryan, 2008). Although personality is referenced, it still presents a universal view, or grouping, of individuals as having like-minded approaches to what could be individually differentiated psychological traits. This could be expressed in the concept of "autonomy," as different psychological profiles have contradictory perceptions of this trait, in particular. Although organizational alignment based on individual personality is not a component of this theory, it does have credence in the application of behavioral factors as incentives from an employer. This provides employers with theoretical viewpoints to address employee behavior through the incorporation of extrinsic coercive controls or the nurturing of internal intrinsic goals (Olson & Maio, 2003). The Self-Determination Theory presents motivation as the result of intrinsic and extrinsic factors related to individual competence, autonomy, and relatedness (Deci & Ryan, 2008). It defines competence as the ability to accomplish a given task, autonomy as the ability to drive one's own actions or destiny, and relatedness as the importance that the individual has to others around them and relationships with others in that sphere of influence (Ryan & Deci, 2000). This theory begins to provide a basis for motivation as a part of personality; however, it still presents a universal view, or grouping, of individuals as having like-minded approaches to what could be individually differentiated psychological traits.

In other theories, such as in the Agency Theory, the author presumes that all individuals possess a universal trait, such as, egoism (Jensen, M. C.; Meckling, 1976; Mitnick, 1976). This causes predictions throughout the model to revolve around individual selfishness. This establishes the presumption that all leadership and shareholders are imbalanced and egotistical and require the introduction of laws to limit abuse. Agency Theory bases production and performance on egoism and decisions that would support an individual's or group's self-interests. This provides predictors for shareholder or executive decisions, as they would base their decisions on whatever outcome most benefited their own needs or desires. This process applies at a high level within the organization, as the agents are often regarded as executive officers or directors, while the principals are regarded as shareholders (Shapiro, 2005). This attribution of traits to high-level leadership is intentional; however, it may be improperly used to define relationships between staff and management. This model is further complicated in that the agent is in a position of greater power, requiring additional incentives to be contributed by the principals during negotiations. It seems clear that not all individuals are egoists, as indicated by social order and psychometric analyses. If egoism is not a motivating factor for all individuals, additional constraints on behavior would have a crushing effect on many personality types. This is another theory that introduces psychology that may be orthogonal or opposed to its actual applied potential. This presents another view of individual personality traits on career performance; however, it has limited application to the variation of individual interests in cybersecurity.

Additional theories establish several other factors as significant to employee success. The Met Expectations theory places employee satisfaction on their individual interpretation of what they expect from a career and what they actually experience (Porter & Steers, 1973). In this model, the employees' expectations were the driving factor in influencing turn-over decisions (Holtom et al., 2008; Joseph et al., 2007). Before this theory was published, in 1972, Lyman W. Porter and Richard M. Steers wrote a literary review called Organizational, Work and Personal

Factors in Turnover and Absenteeism. This presented individual concepts of expectation as a significant factor of satisfaction and retention (Porter & Steers, 1973). The theories of Self-Determination Theory (Deci & Ryan, 2008), the Met Expectations theory (Porter & Steers, 1973), the Withdrawal Model (Hulin, 1991), and the Agency Theory (Jensen & Meckling, 1976; Mitnick, 1976) aligned all individuals to specific traits (Holtom et al., 2008; Hom et al., 2017; WeiBo et al., 2010). This presented a unified personality for all employees that would be impacted in a predictable pattern. They approached personality from a collective viewpoint, seeing all workers as sharing goals and desires. Variation of approach was required within organizational management to move the employee's satisfaction.

The collective personality models are considered less applicable within the Integrative Adaptation and Withdrawal Model (Hulin, 1991). The author, Charles L. Hulin argued that attitude and behavior may be insufficient when predicting individual satisfaction (Hulin, 1991). He proposed that individual behavioral factors needed to be profiled to determine proper courses of action to improve satisfaction and retention (Holtom et al., 2008; WeiBo et al., 2010). Behavioral modeling involves individual inclinations and profiling, as in consistent with this research; however, the methods still fell short of interpreting individual personality factors or interests as primary indicators or satisfaction. Although the Integrative Adaptation and Withdrawal Model did not fully address individual interests, a variation of the theories above presented expectations as the predominant motivator (Hom et al., 2017). Jackson's Taxonomy of Vocational Interests (Jackson et al., 1984) and The Taxonomy of Difficulties in Career Decision Making (Gati et al., 1996) began the investigation into the classification and alignment of individual personality traits to functions. A high degree of consideration is given to Jackson's Taxonomy of Vocational Interests. This work attempted to associate individual preferences in psychological clusters that related to college majors through the Jackson Vocational Interest Survey (JVIS). Jackson was able to demonstrate that there are associations between individual psychology and college major selection. Jackson defined 34 basic interests that were reduced to 10 occupational themes (Jackson et al., 1984). Through a Basic Interest Profile, he associated the interests and themes to several career fields. Although the premise is well-founded, the occupational data used for various job descriptions and the limited temporal relevance of any associations reduced the applicability to a short period of time (Jigău, 2007). This chrono-centrism unfortunately predates the advent of Sir Tim Burners-Lee's vision and design of the World Wide Web (WWW) that became mainstream in 1995, and also the development of a majority of the cyber aspects of information security that followed closely thereafter. Furthermore, as technology is neither the focus, nor is it a historically relevant factor for cybersecurity during that period, direct relevance to today's cybersecurity professionals is relegated to only general concepts. Specifically, Jackson's tests for internal consistency and inter-correlation of individual interests are seen as credible in the development of categories or taxonomies of interests as seen with other interest scales (Taylor & Campbell, 1969). From a different viewpoint, another method of categorizing career decisions arose. The 44 Difficulties in the Elaborated Theoretical Taxonomy by Gati looked at career decisions from the standpoint of individual knowledge about a career and the individual's inability to make a decision concerning a career (Gati et al., 1996). This included concepts that included general personal traits, fear of obligations, what abilities would be required at that moment and in the future, and a lack of knowledge about the career itself. Gati's viewpoint delved into the individual's decision-making process, and how general aspects of personality would influence that process (Gati et al., 1996). The Taxonomy of Difficulties in Career Decision Making emphasized the both the intrinsic and extrinsic struggles that individual's encounter during a career decision (Gati et al., 1996). This is useful in understanding the difficulty that was encountered when creating a taxonomy; albeit, in generalities that have limited implication for identifying interests relevant to cybersecurity career fields.

The variation between The Taxonomy of Difficulties in Career Decision Making and Jackson's Taxonomy of Vocational Interests allows for a plethora of viewpoints surrounding the determination of individual interests (Gati et al., 1996; Jackson et al., 1984). Largely, a subject profession or target career was established, then, individual traits and interests where defined therein. This subjective approach fit nicely with the end goal of this research to identify what interests would align with various functions within cybersecurity; however, there was a dearth of research found that applied to the specific concept of interests to cybersecurity. It was also determined that the interests selected in the various models were not cybersecurity-specific.

The traits expressed in the Job Characteristics Model expressed personality traits related to employee satisfaction (Hackman & Oldham, 1976). Variety involves the changeability within one's position and function. Identity involves the ability to realize an outcome in one's work; a completion or finished product derived from one's efforts. Significance relates to the level of impact the work has on people or the organization. Autonomy describes the extent to which an employee has personal oversight into their work and outcomes. Feedback is the amount of reporting provided to the employee while conducting, or after completing, their work (Lunenburg, 2011). While all of these traits are significant factors in satisfaction, they may be seen as more general in their application. The broad concepts that may be taken from the Job Characteristics Model are how traits combine with employer-related functions: "Variety," "Significance," "Autonomy," and "Feedback," with a seemingly personal function, "Identity (Joseph et al., 2007)." The occupational position presents the employee with both the former and latter functional attributes as standards of employee satisfaction. This is a holistic view placed on each employee regardless of their inherent personality type. This model tended to focus on psychological diversity in the sense that the factors are not universal. An employee's psychology, whether the result of nature or nurture, defines if they would crave feedback or silent validation, autonomy or interdependence, variety or consistency, or any other trait. This creates a model that would adjust the attention given to the respective trait in order to improve overall employee satisfaction and performance without regard to the individual psychology Table 3-4 MPS Formula.

Table 3-4 MPS Formula

$$\boxed{\text{MPS} = \frac{\text{Skill Variety} + \text{Task Identity} + \text{Task Significance}}{3} \text{ X Autonomy X Feedback}}$$

Note. From Job Characteristics Model (Hackman & Oldham, 1975)

The Motivating Potential Score (MPS) positions the autonomy and feedback traits for greater influence into the personal satisfaction of the individual employee. This formula would be accurate for every employee that exhibits personality traits that positively support these measurements; however, this would render a false-positive result for employees exhibiting the contrary individual traits, as discussed above. The model successfully presents researchers with factors that acknowledge employee psychology as an aspect of job satisfaction. This does not provide a causal relationship based on variations in individual psychology to determine performance or retention; however, it does effectively reference personality as an area of consideration for employee satisfaction and retention (Lunenburg, 2011). The Job Characteristics Model introduces personality traits as an influence for performance and satisfaction; however, it constrains the personality values to predefined traits that are considered advantageous for every employee: Variety, Identity, Significance, Autonomy, and Feedback (Ghapanchi et al., 2013). This presents a potentially contentious precedent, as some of the subjects evaluated under this model will have a positive outcome not because of the validity of the model, but because of the chance that the model fits their individual personality traits. Other individuals will be misinterpreted as unhappy due to organizational structure, not individual preferences that were different than expected. As an example, researchers can conduct investigation into individual outcomes for the trait, "variety." Empirically, the personal trait, "variety," is positively valued under several different personality types. Because the variety factor is inappropriately applied as universally positive, it will generate erroneous results. Some results will be positive, others negative, as this factor is not the independent variable for the dependent variable of satisfaction or performance, it is only a mediator to explain the preferences of a particular personality trait. As this example has indicated, the Job Characteristics Model presumes that all individuals will have a better chance of retention or satisfaction if they experience variety within their work (Hackman & Oldham, 1976). A majority of the population may enjoy radical variability in their job, but this does not indicate that "variety" is a fundamental aspect of satisfaction or retention. It certainly does not indicate increased levels of performance, as variety would invariably introduce uncommon tasks to the employee, generating additional contemplation over the correct solution; thereby, reducing productive workflow. As with the prior theoretical foundations, the Job Characteristics Model presents a solid foundation for subjective identification of personality traits as influential to career output; however, any identification with cybersecurity or individual interests is not given.

3.2.2 Challenges and Advancements in Psychometrics

Formal literature offered a number of general systems and models that were incorporated to begin the design of a specific taxonomy of interests as they applied to cybersecurity (Gati et al., 1996; Jackson et al., 1984; Kaufman et al., 2013; Nickerson et al., 2009). The limitations were seen in the specificity and application to both functions and career interests. In order to arrive at greater clarity for how to design a system that would allow for interests that were specifically related to cybersecurity, a subset of psychometric analyses was investigated. Primarily, the divergence from an individual's psychological traits to a representation of their personal interests was pursued, as this was seen as the best method to align cybersecurity functions. Throughout this study, psychological traits are seen in their form as conceptual taxonomies. The goal of this research is to develop an alignment between individual interests and cybersecurity functions, not to create a psychometric profile that would base career selection on inherent psychological traits. As such, this research used the psychological and personality traits discussed in psychometric profiling solutions to better hone a list of cybersecurity-related interests. Psychometric profiling became an indispensable tool in understanding the processes by which interests and psychological traits were defined (Kennedy et al., 2014; Tokar et al., 1995). Beyond psychometric profiling, solutions that directly addressed career interest alignment were investigated (Jigău, 2007). The resources lacked insight into cybersecurity-specific functions; nonetheless, they were useful in understanding design methodologies.

Psychometric profiling was especially helpful, as profiling helps subdivide personalities into discrete segments, allowing the application of personal traits to potential outcomes (Goldberg, 1999). Although this research does not implement a psychometric, an adequate understanding of how psychometric tools evaluate individual personality to discrete outcomes is foundational to the proper development of an individual career interest survey and artifact. Research was required to determine the caveats of psychometric testing to properly determine how the test results would relate to a particular trait, condition, or situation of employment. This led to research concerning the congruity between psychometric examinations that provided both links to other profiles and complimentary theories surrounding individual interests (John et al., 2008). These additional references created the need for methods by which they may be analyzed more clearly. To attain additional clarity, categories were developed to better define psychometric profiles to be used as a representative foundation. This provided a focused definition for each category of psychometric model, allowing an investigation into potential correlations in a succinct manner through the use of representative texts relating to each of the developed categories. This investigation is the basis for the development of an Individual Interest Inventory (III) that directly relates to cybersecurity job functions. This new artifact is not a psychometric, but a profile of individual interests. This does not preclude the development of a specific psychometric in future derivative research artifacts, but that process would be out-of-scope for this particular study.

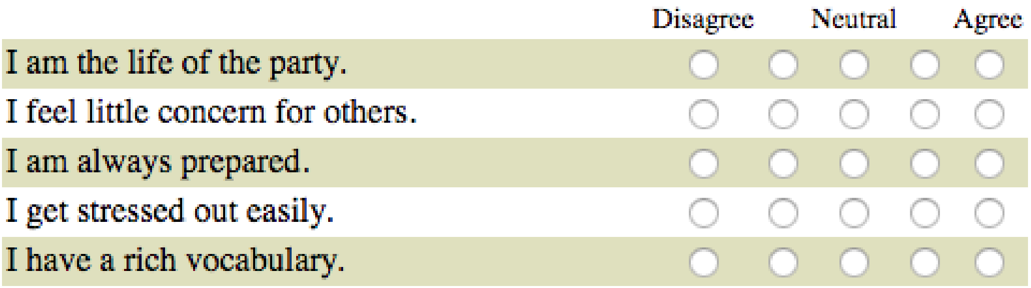
To begin the study into psychometric categorization and definitions, a small subset of popular psychometric analyses was selected. The Five Factor Model (FFM) (Digman, 1990; Goldberg, 1990; Norman, 1967), the Jung Typology (Jung, 1921; Kelland, 2017) and Myers-Briggs Type Indicator (MBTI®) ((Myers, 1962/2016)) and the Holland Codes (RIASEC) (Holland, 1986) were seen as descriptive from broad to increasingly narrow, respectively. Although valid psychometric results may be attributed to a subject without formal research methods due to the existence of previously validated testing instruments, it is important that the researcher understands the testing process to allow for the creation of a novel approach. This is underscored in the development or usage of existing tests in new ways or in combination with other instruments, as many researchers relied on purely quantitative results of analysis that resulted in improper attribution of psychological traits (Goldberg, 1998). In some cases the data may seem random from a purely quantitative viewpoint, requiring additional methods and applications of original thought to understand the actual meaning behind the output. One area where quantitative data are seemingly random across varied subjects is identified as a misinterpretation of the testing language by each subject (Dawson & Thomson, 2018). The language itself then becomes an aspect of the examination, as indicated by Osgood's Semantic Differential Technique (Klement et al., 2015). Language may be the factor that is influencing the outcome of the psychometric data, not the actual meaning of the test. In the creation of a library or taxonomy of interests as they apply to cybersecurity, much of the terminology was already understood by the narrow community involved. Additional considerations for psychometric testing involve influence by several environmental and social factors ranging from technological capabilities, to personal bias and even political associations (Holland, 1986). In the absence of, or through calculated bias, analyses can be useful as predictors of behavior; however, proper care must be taken to ensure that the subject understands the terminology and contextual meaning of the test being administered (Norman, 1967). This allows both the subject and researcher to achieve accurate results for qualitative or quantitative research across numerous disciplines. Alternatively, career interest profiles may allow for the use of conventional, unambiguous language that directly relates subject responses to allocated outcomes. It is important to note that psychometric profiles provide insight into the psyche of individuals and the sociological phenomena of a group that extends beyond what might relate to cybersecurity functions. They are often investigating aspects of humanity that span beyond conventional experiences (Kaufman et al., 2013). This broad interpretation is outside of the scope of this research, as cybersecurity-specific interests require a narrower focus. Psychometrics, as a whole, are examining other aspects of an employee's mind, not specifically their individual interests (Morgeson et al., 2007). This is both seen in materialistic tradition where personality factors are considered as a separate and measurable state as a result of personal experience and genetics, as well as holistic approaches that investigate a spiritual factor involved in personal foundations of morality and decision (Kelland, 2017). As much as psychometric investigation is useful, it is often analyzing aspects of employee psychology that are outside the scope of this study; however, these models are informative in understanding the design of profiles that predict or prescribe individual purpose and action.

Five Factor Model (FFM) Psychometric

The Big Five Personality Traits Test or the Five Factor Model (FFM), often known as the "Big 5," summarizes personality traits using a lexicon of adjectives, and groups personality types into five factors (Digman, 1990). Digman performed three studies in Japan, the Philippines, and Germany and came to the resolution that the five-factor model is a good solution for personality testing that surpassed linguistic barriers. An example of the FFM test is provided below, Figure 3-2 IPIP Big Five Factor Markers,

Figure 3-2 IPIP Big Five Factor Markers

Procedure: The test consists of fifty items that you must rate on how true they are about you on a five point scale where 1=Disagree, 3=Neutral and 5=Agree. It takes most people 3-8 minutes to complete.

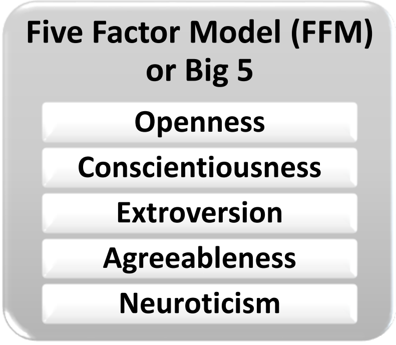


	Disagree		Neutral		Agree
I am the life of the party.	○	○	○	○	○
I feel little concern for others.	○	○	○	○	○
I am always prepared.	○	○	○	○	○
I get stressed out easily.	○	○	○	○	○
I have a rich vocabulary.	○	○	○	○	○

Note. From (Digman, 1990).

In 1884, Sir Francis Galton wrote Measurement of Character, where he developed what is now known as the Lexical hypothesis to study personality (Galton, 1884). Galton used Roget's Thesaurus in his trait research and composed a large list of adjectives/traits that describe personalities (Revelle, 2014). The idea of the Lexical Hypothesis is that the language of a culture will naturally use words that describe personality, and the most important words used to describe personalities will be summarized by a single word. This is similar to the way cybersecurity-related interests may be codified. The FFM uses adjectives to define psychological traits, see Figure 3-3 Five Factor Model (FFM) Personality Types).

Figure 3-3 Five Factor Model (FFM) Personality Types



Note. From (Digman, 1990).

Openness to experience represents an individual's inclination to curiosity or consistency. Conscientiousness describes an individual's tendency to also be associated with consistency and focus; however, this aspect is within the realm of spontaneity versus fundamentalist self-discipline. Extroversion defines a person's tendency to be outgoing and energetic or reserved and quiet. This also entails a personal assertiveness that could overlap with conscientiousness. Agreeableness defined an individual's predilection for cooperation instead of competition. This trait may also involve aspects of conscientiousness in self-discipline and with extroversion in assertiveness. Neuroticism expresses the subject's self-image through confidence or anxiety. Individuals with high levels of neuroticism can result in a lack of compassion and are considered less emotionally stable (Digman, 1990).

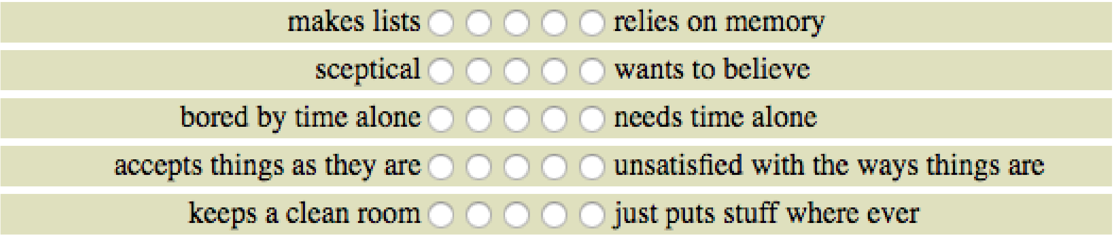
Due to the overlapping of several of the aspects of the FFM, some organizations have selected a subset of Conscientiousness, Agreeableness, and Neuroticism as a clearer determinant of psychometric result. Although some of these traits have been useful in the determination of general career success and performance (Chamberlain et al., 2005), the reduction of the FFM into three traits is possibly an indication of the complexity of human personality and the inability to precisely define qualities of human behavior. This inability to align innate human psychology to specific career is an indication that psychometrics may lack the ability to define an individual interest correlation. As there are instances of ambiguity within the FFM with regards to specific personality-to-function interrelation, it may be necessary to use the model as a more general tool to provide initial personality evaluations at a broader level (McAdams, 1992). This would indicate that the FFM should be included in derivative research as a model of broad usage, as it lacks the ability to specifically identify personality traits in a programmatic manner that would have individual application to cybersecurity or other career functions; however, this may also be true for each psychometric analysis.

Jung Typology and Myers-Briggs Type Indicator (MBTI®) Psychometric

The Jung Typology represents personality in eight distinct modes (Jung, 1921; Kelland, 2017). It was augmented by Myers-Briggs to include additional traits that extended the Jungian Typology to a total of sixteen individual traits (Myers, 1962/2016). This is both representative of the Extended Jungian Typology and Myers-Briggs Type Indicator evaluations (see Figure 3-4 Open Extended Jungian Type Scales 1.2).

Figure 3-4 Open Extended Jungian Type Scales 1.2

Procedure: This test has sixty items in two sections. In the first section, each of the items consists of two opposing personality descriptions (e.g. honest ..... dishonest) put on two the extremes of a five point scale. For each item the subject must select an interval on the scale that best reflects their personality; from all of one, to a mix of the two, to all of the other. In the second section, the subject is given items in the first person (e.g. "*I love ice cream.")* and asked to rate how much they think each is true. It should require approximately five to seven minutes to complete the test.



makes lists ○ ○ ○ ○ ○ relies on memory

sceptical ○ ○ ○ ○ ○ wants to believe

bored by time alone ○ ○ ○ ○ ○ needs time alone

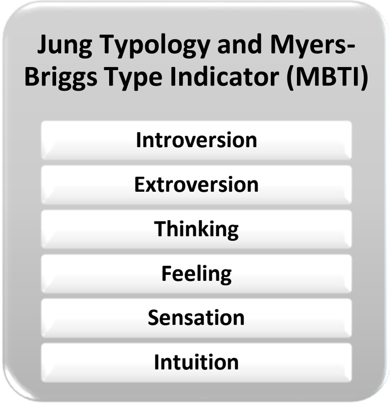
accepts things as they are ○ ○ ○ ○ ○ unsatisfied with the ways things are

keeps a clean room ○ ○ ○ ○ ○ just puts stuff where ever

Note. From (Jung, 1921), (Myers, 1962/2016).

There are many variations in psychometric examinations, as such, Open Extended Jungian Type Scales 1.2, will be used as a common example for the purpose of this research. Further reference to the MBTI®, unless otherwise noted, will be in reference to this particular test. Jung felt that personality types were difficult to identify subjectively; however, he also determined that there are certain ways humans react, and through understanding the general ways in which individuals relate to the world, it is possible to understand the dynamics of their relationships and personalities. This theory, called, "The Psychology Of Consciousness," is the basis for the Jung typologies (Jung, 1921). This is similar to the way that individual interests may be defined to correspond to a particular outcome. Jung Typology and Myers-Briggs Type Indicator (MBTI®) Psychometrics Carl Jung proposed eight personality types composed of two attitude types and four functions (see Figure 3-5 Jung Typology Traits).

Figure 3-5 Jung Typology Traits



Note. From (Jung, 1921), (Myers, 1962/2016).

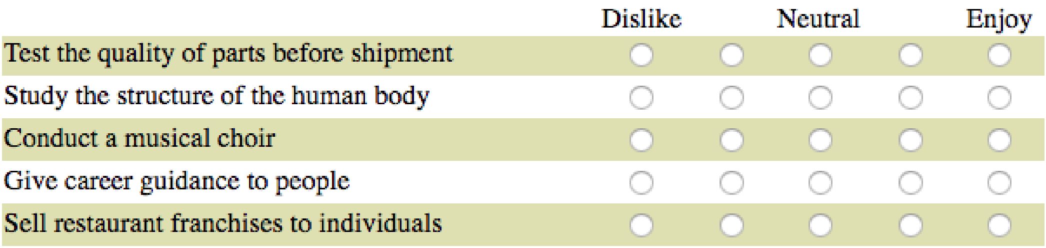
The concepts within the Jung profile are similar to the FFM. Introversion and extroversion represent the method by which an individual gains energy and operates in society. Sensation and intuition involve the manner by which an individual gains information. Sensing individuals readily received external recommendations, while intuitive individuals lean more heavily on their own understanding. Thinking and feeling involve the method by which we make decisions. Feeling individuals make decisions based on their value systems, while thinking individuals make decisions based on objective analysis or rules (Jung, 1921). The Myers-Briggs Type Indicator (MBTI®) incorporated the additional traits of judging and perceiving. The incorporation of these two traits expanded the list of eight traits to sixteen. Although sixteen traits were identified, the original eight typologies were still in effect. This can be illustrated in the addition of a judging or perceiving aspect to each of the existing traits. The judging and perceiving traits involve the individual's tendency to follow a rigid schedule as a judging individual or manage ambiguity and a lack of structure as a perceiving individual (Kelland, 2017). Jung discussed the impact of extroversion and introversion on a scale best-suited for a general identification of adaptation to what seems to be a procedural focus, not a specific task or function (Jung, 1921). This attribute would tend to place the Jung and MBTI® on a more specific tier than the FFM; nonetheless, this was still too ambiguous for specific vocational functions. This further illustrates the need to account for traits that are specific to cybersecurity functions.

Holland Codes (RIASEC) Psychometric

John Lewis Holland, a psychologist, profoundly influenced vocational psychology by developing and creating the career development model called the Holland Occupational Themes (Holland, 1986). This typology, which is also called the Holland Codes, or RIASEC, is unique because it simplified the process of psychometric testing and has directed countless individuals to a career (McDaniel & Snell, 1999). Since there are many variations of this test, the IIP RIASEC Markers test, Figure 3-6 IIP RIASEC Markers, will be used as a common example for the purpose of this research (Liao et al., 2008).

Figure 3-6 IIP RIASEC Markers

Procedure: The test consists of 48 tasks that you will have to rate by how much you would enjoy performing each on a scale of (1) dislike (2) slightly dislike (3) neither like not dislike (4) slightly enjoy (5) enjoy. The test will take most five to ten minutes to complete.



	Dislike		Neutral		Enjoy
Test the quality of parts before shipment	○	○	○	○	○
Study the structure of the human body	○	○	○	○	○
Conduct a musical choir	○	○	○	○	○
Give career guidance to people	○	○	○	○	○
Sell restaurant franchises to individuals	○	○	○	○	○

Note. From (Liao, 2008).

He first introduced his theories in 1959, and then over the course of many years, even after retirement, Holland continued developing his typologies aligning a person's personality to their vocation (Rayman, 2008). Holland was tasked with technical evaluations of personality and vocation that relied on empirical data. Through a robust and open system that allow continuous updates, Holland's Codes were able to take psychological qualities and accurately describe them into a discrete codification (Holland, 1986). Holland's Codes or the RIASEC Model is composed of the following identifiers, (see Figure 3-7 Holland Codes (RIASEC)).

Figure 3-7 Holland Codes (RIASEC)

Holland Codes (RIASEC)
Realistic
Investigative
Artistic
Social
Enterprising
Conventional

Note. From (Holland, 1986).

The realistic trait identifies individuals who would like to work with physical components or concrete results. The investigate trait identifies individuals who would study how or why a system or entity works. The artistic trait identifies personalities that enjoy the arts and creativity. The social trait corresponds to a desire to help others. The enterprising trait defines individuals who would like to lead or manage an organization or business. Finally, the conventional trait identifies individuals who would be most happy with consistent and repetitive work (Lewis & Rivkin, 2000). Even though RIASEC provides the most specific analysis of the psychometric analyses reviewed, it contains underlying psychological traits that are unrelated to cybersecurity functions.

3.2.3 Proposition 02: Taxonomy of Interests

Throughout the literature there was little to no mention of cybersecurity functions or interests that relate to cybersecurity careers. Jackson's Taxonomy of Vocational Interests was the most closely identifiable source of interest to career alignment; however, Jackson, similar to Holland, did not investigate individual functions, but instead focused on what might be called industry segments. The psychometrics delved deeply into human psychology to bring method or meaning to innate human traits. The congruence between the psychometric analyses were seen to have a form of inter-correlation; however, they were not adequately aligned to cybersecurity or cybersecurity functions and tasks. This lack of resource for both a focused interest library and a taxonomy of interests that align with cybersecurity functions presented an inability to answer what interests would be of use or how to categorize cybersecurity-specific interests. This required the development of a specific taxonomy of interests that would align directly with the cybersecurity profession. This development would aid in the purpose of this research to develop an interest-to-function alignment model to support cybersecurity professionals and organizations.

Proposition 02: Taxonomy of Interests

Therefore, this research proposes the development of a specific taxonomy of interests that would align directly with the cybersecurity profession.

3.3 The Alignment of Interests-to-Functions within Cybersecurity (Artifact 03 / Proposition 03)

Specific tasks and organizational processes are only advantageous to individual satisfaction and performance when those tasks or situations are properly aligned with the individual's interests (Campbell, 2008). Not all individuals desire the same levels of feedback, solitude, or autonomy that are often associated with individual satisfaction (Hackman & Oldham, 1976). The proper alignment of an individual's interest-to-function will also cause an improvement in performance (Tett & Jackson, 1991). An understanding of psychological factors, individual interest inventories, career functions, and satisfaction models is critical to the development of an interest-to-function alignment model (Bartenschlager & Goeken, 2009; Onita & Dhaliwal, 2011). It became necessary to determine a model for properly aligning individual interests to cybersecurity career functions. Job retention models provided frameworks from which organizations and employees garnered support for corporate or individual policies and activities for the goals of increasing performance and satisfaction, and subsequently, retention (Heavey et al., 2013; Holtom et al., 2008; Hom et al., 2017; WeiBo et al., 2010). These models presented both a mechanistic view of employees within an organization, as cogs in a machine, as well as realizing psychology as a pertinent factor. In cases of the latter, where employees are seen as psychological beings, models were found to define psychological influences in terms of performance or satisfaction; however, the psychological markers or traits were statically defined as universally shared, or collective, psychological goals. Most frequently, a "one size fits all" solution is designed around psychological traits with a disregard for the wide variation of intrinsic character that is found in practice. This ignores the actuality that individual preferences may vary greatly from one person to the next. This research delves into the alignment of the earlier function and interest taxonomies to create a model that defines how cybersecurity functions align with individual interests. (see Table 3-5 Key Theories and Concepts for Interest-to-Function Alignment: Proposition 03).

Table 3-5 Key Theories and Concepts for Interest-to-Function Alignment: Proposition 03

Theory	Key Concepts	Relevant Aspects of Theory
Intermediate Linkage Model **(Mobley, 1977)**	Job satisfaction Turnover links	Provided some process overview for alignment operations.
IT Career Paths **(Joseph et al, 2012)**	Satisfaction in career Individual profiles	Individual profiles are broadly integrated through case studies that involved retention, pay, knowledge, skills, and organizational factors.
IT Turnover Theory **(Joseph, 2007)**	Interest and function alignment Employee turnover	Individual factors were integrated with organization factors to provide a model for turnover intention.
Job Embeddedness Theory **(Mitchell and Lee, 2001)**	Why people leave Socialization tactics	Individual interests were already defined in terms of what community or team functions would be advantageous.
Personality Dimensions **(Judge et al., 1999)**	Predict career income Predicts job satisfaction	The usage of a psychometric to predict career satisfaction. The reduction of personal interests to a limited set of factors.
Theory of Organizational Equilibrium **(March and Simon, 1958)**	Employee feelings and satisfaction Organizational incentives	Employee satisfaction from a broad scope within a collective mindset.
Turnover Model **(Steers and Mowday, 1981)**	Steps involved with voluntary employee termination Employee Turnover	Organizational commitment questionnaire concerning voluntary employee turnover.

Note. The key concepts and relevant aspects of the seven theories used to develop Proposition 03 and Artifact 03 are provided for a brief overview and reference as well as a foundation for the development the Interest-to-Function Alignment Model.

3.3.1 The Problem of Classifying Individual Interest to Cybersecurity Function in Academic Literature

At this point, the challenge of aligning individual interests to cybersecurity functions was clear. Neither interests nor functions where found to be adequately defined in the academic or vocational literature reviews (Ghapanchi et al., 2013; Ghapanchi & Aurum, 2011; Joseph et al., 2007, 2012). As such, both of the prior propositions established the need to categorized cybersecurity functions and individual interests in a way that would allow for the alignment of both concepts. To aid in the development of the desired alignment, methodologies from several well-established theories were incorporated with vocational resources. Initially, theories related to employee satisfaction within organizations were investigated (Hardigan et al., 2001). In one case, employee satisfaction was seen through the concepts of contributions and benefits. As long as the employee felt that there were adequate incentives, they would be satisfied and desire to stay (J. G. March & Simon, 1958). Again, this theory approached employee satisfaction from a broad scope within a collective mindset that could not be satisfactorily aligned to individual interests or cybersecurity functions (Holtom et al., 2008; Joseph et al., 2007; WeiBo et al., 2010). Although the theories investigated were now concerned with employee perception, there was a theoretical misalignment that continued. This included the concepts from the Turnover Model; however, the organizational commitment questionnaire was useful in the construction of this study’s survey (Mowday et al., 1979). The Intermediate Linkage Model (Mobley, 1977) that broadly discussed the employee's process of making a leave or stay decision that provided some process overview for alignment operations, but fell short of cybersecurity function (Heavey et al., 2013; Holtom et al., 2008; Hom et al., 2017; Joseph et al., 2007; Singh & Sharma, 2015; WeiBo et al., 2010). This can also be seen with models that discussed employee retention and satisfaction through community involvement (Allen, 2006; Mitchell & Lee, 2001). In those situations, individual interests were already defined in terms of what community or team functions would be advantageous.

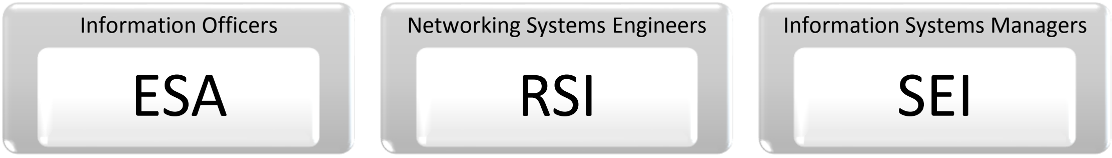
The focus was narrowed to technology-oriented satisfaction and retention theories in hope that they would provide greater potential to supply this study with alignment foundation (Ghapanchi et al., 2013; Joseph et al., 2012). IT Turnover Theory was examined for aspects that would be integral to both interest and function alignment (Joseph et al., 2007). In this case, individual factors were integrated with organization factors to provide a model for turnover intention (Joseph et al., 2007). This model built upon March and Simon's model to provide for greater influence of individual factors (Simon, 1969/1996). Although this provided a structural model for IT turnover intention, it did not provide detail for individual interests or cybersecurity functions. This is also true for "Personality Dimensions of Career Success" in relation to specific cybersecurity functions (Judge et al., 1999). In Judge, et al.'s study, individual personality factors were taken from a broad psychometric profiling tool, the Five Factor Model, and aligned to career success factors (Judge et al., 1999). This was, again, touching on the concepts of interest-to-function alignment; however, it was interested with general success factors, not specific interests, and certainly not specific interests as they align to cybersecurity functions. In 2012, Joseph, et al, revisited the satisfaction and career mobility theme with additional research into individual profiles; however, the interpretation of individual profiles was broadly integrated through case studies that involved retention, pay, knowledge, skills, and organizational factors. The individual profiles did not address individual interests that would align to cybersecurity functions.

3.3.2 Challenges and Advancements in Vocational Alignment

Numerous vocational and journal resources were investigated to help define alignment strategies for individual interests to cybersecurity functions (Campbell, 2005). The most closely related articles relating to alignment were the Jackson's Taxonomy of Vocational Interests (Jackson et al., 1984) and Holland's Vocational Interest Inventory (Holland, 1986). These resources were already useful in the attribution of function and individual interest; albeit, they both were inadequate when discussing cybersecurity functions and interests that align with those functions. To disambiguate the concept of alignment, this research will consider alignment in the simple sense that two traits or subjects may be associated with one another by some metric. This avoids the concepts of organizational alignment between IT and the organization as a whole (Chan, 2002) or the inability for some organizations to align their processes within a single department (Onita & Dhaliwal, 2011). This study does benefit from the various levels of technical governance and policies that relate policy to human behavior; however, this is limited in scope to a specific policy and employee behavior (Schlosser et al., 2015).

Even the most specific psychometric, the Holland Codes, did not adequately align relevant interests to cybersecurity functions (Holland, 1986). Holland was able to be specific for several career functions, as he believed that the tests were not complete without an appropriate correlation to a career aligned with the RIASEC code. As such, he established a list of careers corresponding to the RIASEC scores, called the Dictionary of Holland Occupational Codes to link the codes directly to a career (Holland, 1986). This has been one of the largest contributions from Holland because once the personality type has been revealed, the results of the test are directly correlated to specific careers, defined by the 3 letter RIASEC code (Nauta, 2010). In other words, the person’s personality RIASEC code is matched to the correlating occupational RIASEC code. The figure below, Figure 3-8 Sample Job Titles and RIASEC Code, provides a few sample Information Technology jobs and their corresponding RIASEC Code.

Figure 3-8 Sample Job Titles and RIASEC Code



3.3.3 Proposition 03: Alignment of Interests to Functions

The previous section has provided the foundational concepts by showing the literature analysis and reviews of the previous work on cybersecurity, psychometrics, and the foundational theories. Theories involving employee performance, satisfaction, and retention will always be subject to the infinite number of factors that may influence them. This makes a perfectly holistic unification of all factors involved impossible to construct, relegating this research and prior research to small collections of factors contained within specific arenas impacting satisfaction, performance, or retention. Although the insights and knowledgeable investigation that each researcher put forth in their work provided a solid foundation for the development of this study, there remained a consistent gap between defined cybersecurity functions, the interests that would align to those functions, and the combination of the taxonomy of functions and interests that create a relationship between the two.

Proposition 03: Alignment of Interests to Functions

Therefore, this research proposes the combination of the taxonomy of functions and the taxonomy of interests to create an aligned relationship between the two.

3.4 Sociotechnical Systems in Cybersecurity

A Sociotechnical System (STS), disambiguation from Science and Technology Studies (STS), is a concept that acknowledges the social impact of technological systems. This is not to reduce the concept to merely the impact created by technical systems in society, but to express that society works with technology to achieve goals, and this interaction affects the way society acts and thinks (Malatji et al., 2019). This involves the environmental, social, and technical solutions that must work mutually to achieve society's functions (Malatji et al., 2019). Ranging from the 1950's with British coal mining research and in the 1970's with Fred Emery's work to recent articles regarding the impact of sociotechnical systems within cybersecurity in society, the topic of how society is affected by technology is far-reaching (Emery, 1982; Stevens, 2018; Trist, 1981). In healthcare, human impact has always been a consistent focus of the industry. As the healthcare industry integrates more completely with technology, the sociotechnical impact of this interaction becomes more evident. This can be seen in security and privacy, as well as the increased availability of services (Shahzad et al., 2017). Within the realm of Information Systems, there is still a great deal of work to do involving the realization that measurements of social impact should be fully considered with the implementation of technology. This need is being addressed in recent work through the construction of models to measure the sociological considerations within technical systems, as well as the work that conducted to define which technical frameworks take sociological impact into consideration (Alter, 2010; Bostrom et al., 2009; Malatji et al., 2019; Wu et al., 2015).

The rapid expansion of concern and revelation concerning the topic of sociotechnical impact has generated some misunderstanding or alternative viewpoints. This is especially true when viewed in context of cybernetics, and even, cybersecurity systems. In the case of cybernetics, the technological term coined in 1948 by Norbert Wiener (Wiener, 1948/2019), the constraint of the technical-human interaction is on a more personal scale. When examined, the word, "cybernetics," now often reduced in form to a shorted form, "cyber," has within its meaning that both humans and technology work together through manual and automated processes to achieve human objectives. This is similar to the mutual affect that occurs within sociotechnical systems, but differs in the conceptual scale and focus of the symbiotic relationship. Cyber systems reflect a scale that involves humans and automated machines operating on a particular task or industry. This differs in sociotechnical systems in the concept of a universal condition that all, or a portion, of society is affected by technology and has a mutually symbiotic relationship, whether consciously realized or not. Cyber systems are also focused on the ability of automated controls to make independent decisions as well as decisions directed by the human controllers. In sociotechnical systems, automatic and manual behaviors are not seen as separate differentiating factors within a sociotechnical structure. There is also some evidence in the literature to illustrate that in some cases, sociotechnical systems are not considered an envelope for cybersecurity systems, but an enclosed part of cybersecurity systems (Stevens, 2018). Does the concept of cybersecurity encompass sociotechnical systems, or do sociotechnical systems encompass the concept of cybersecurity? Within this study, cybersecurity is considered to be a part of the greater concept of sociotechnical systems. The sociotechnical concept involves any aspect of social, technical, or environmental impact that may be measured (Malatji et al., 2019). Whereas sociotechnical systems relate to the inter-dependency of society and technology, or the impact of technology on individual lives or those within entire community, cyber systems relate to the shared responsibility for decision-making between, and transcending, humans and technology. Cyber represents the integration of technology into the individual human experience. This concept has expanded to become the augmentation of human ability as well as the enforcement of human will vicariously through technical surrogates. In this case, cyber systems are capable of making decisions based on statistical interpretations of conditional inputs or via artificial intelligence. From a sociotechnical point of view, cyber systems, such as cybersecurity, are a component within the whole of sociotechnology. Based on this interpretation, cybersecurity should be considered within the realm of a sociotechnical system in how human lives are impacted through its usage in society.

3.5 Summary

The purpose of this research is to design an interest-to-function career alignment model for cybersecurity professionals that will enable organizations to increase employee retention and individuals to improve job satisfaction. This involved investigations of job theory and human resource theory for existing career alignment models. It was discovered that the resources required to align cybersecurity functions to individual interests for cybersecurity professionals were inadequate or unavailable. This research also revealed that there exists ambiguity within the cybersecurity industry surrounding a taxonomy of roles and functions. Moreover, individual interests are not applied to cybersecurity functions within existing literature, causing the alignment of a taxonomy of interests to functions to be unavailable. The ambiguity surrounding individual interests and their alignment to specific cybersecurity functions is an area of concern for future sociotechnical system design.

The dearth or absence of existing models required the development of three separate propositions. A table was created to relate each of the propositions to the data collection, qualitatively, as low, medium, or high. Low indicates that the proposition was not discussed in great detail, medium indicates that the proposition was discussed, and high indicates that the proposition was a focal point of discussion. The first prerequisite proposition, the Taxonomy of Job Functions, is supported under each of the expert interviews, surveys, and focus group to either a medium or high extent. These ratings were achieved directly from the respondents' comments. For instance, Appendix D.2 Focus Group Data remarks the need to modify the functional list for a better fit for cybersecurity professionals. The second prerequisite proposition, the Taxonomy of Interests, is not referenced in the Job Functions Survey; therefore, it receives a low marking for that data collection instrument. In the focus group, the experts were willing to share their agreement and suggestions with the second proposition openly, providing a high marking in that category. The final proposition, Alignment of Interests to Functions, was highly supported in the interviews and surveys. This proposition is the primary proposition, exhibiting the alignment of the prior two prerequisite propositions. The ability to gather meaningful data for the final integrated artifact was possible due to the positive data collection from the prior prerequisite artifacts. The specific data collected is covered in detail in the approximately sixty pages of appendices from Appendix C.1 Interview Slides through Appendix D.4 Cybersecurity Interest-to-Function Survey Data.

To aid in visualization, Table 3-6 Support from Data Analysis for Propositions shows support for each proposition from each data collection source. For clarification, the following explanation is provided for the focus group questions and responses. In the case of the focus group, all data are directly related to, and provide strong support for, each of the propositions; therefore, the respective column and row lists support as, "high." These data points are further examined in detail in the appendix for additional review.

Table 3-6 Support from Data Analysis for Propositions

Data Collection Title	Proposition 01: Job Functions	Proposition 02: Job Interests	Proposition 03: Interest-to-Function
Expert Interview: Part 1	Medium	Medium	High
Expert Interview: Part 2	High	High	Low
Confirmatory Interviews	Medium	Medium	High
Focus Group	High	High	High
Job Functions Survey	High	Low	Low
Cybersecurity Interest-to-Function Survey	Medium	Medium	High
Final Survey	Medium	Medium	High

Note. The classifications of low, medium, and high relate to the amount of data from each investigative tool that directly impacted each artifact. The specific impact is discussed in the appendix.

4 Design Principle and Artifact Development

This chapter introduces the three artifacts that were designed, built, and evaluated for this study. The first two artifacts: Artifact 01 - Taxonomy of Cybersecurity Functions, which discusses roles, job titles, and job functions in cybersecurity, and Artifact 02 - Taxonomy of Cybersecurity Interests, which details the individual interests that may be factors within cybersecurity career functions, are used as prerequisite artifacts to create a third integration, Artifact 03 - The Alignment of Cybersecurity Interests-to-Functions.

4.1 Prerequisite Artifact 01 - Cybersecurity Career Functions

The following section clarifies the relationship between design challenges, artifact requirements, and justificatory knowledge. This includes both theoretical knowledge from academic sources together with practitioner publications and resources. The chart provides additional clarity into the artifact development process.

4.1.1 Artifact 01 - Requirements for Cybersecurity Functions

Table 4-1 Artifact 01 - Requirements for Cybersecurity Functions

Design Challenges	**Artifact Requirements**	**Justificatory Knowledge**	
		Theory	**Authors**
		Role Conflict and Role Ambiguity	(Johnson & Stinson, 1975; Rizzo et al., 1970)
		Role Theory	(Biddle, 1986; Katz & Kahn, 1978)
DC01: The plethora of job titles within the cybersecurity industry may indicate immature role development and ambiguity. **DC02**: The functional overlap of several positions causes additional ambiguity of functions within cybersecurity. **DC03:** Business models rely on legal and regulated activity for proper function. **DC04**: Cybersecurity is perceived as manual control of technical systems.	**AR01**: Cybersecurity Titles and Roles should be reduced to a representative subset. **AR02**: Cybersecurity functions should be collected from the subset of roles and further codified into a foundation of discrete functions. **AR03**: Business models need to reflect the existence of a persistent omnipresent cyber threat to operations. **AR04:** Cybersecurity must be seen as a system of systems with both autonomous and individual controls.	Taxonomy Development in Information Systems	(Nickerson et al., 2009, 2010)
		Justificatory Knowledge (Technology Focused) Formal Frameworks[1] • NIST / NICE National Institute for Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) • The ISO27000 Series International Organization for Standardization (ISO) Professional Organizations[2] • International Information Systems Security Certification Consortium (ISC)²® • ISACA® Information Systems Audit and Control Association Training Organizations[3] • The SANS Institute SysAdmin, Audit, Network and Security (SANS) Institute • InfoSec Institute Information Security (InfoSec) Institute Occupational Database[4] • The O*NET Program Cybersecurity Career Websites[5]	

[1] (ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), 2014; Newhouse et al., 2017)

[2] (International Information System Security Certification Consortium (ISC)^2, 2019; Otero, 2018)

[3] (Paller, 2020), (InfoSec Institute, 2020)

[4] (Lewis & Rivkin, 2000)

[5] (Curran, 2016; *Cyber Security Degrees and Careers*, n.d.; *Cybersec Jobs*, n.d.; *Top 10 Security Careers*, n.d.; Department of Computer Science, n.d.; Doyle, 2019; Kaelin, 2018; Morgan, 2016; Security Wizardry, 2018; Zeltser & Hoyt, 2015)

A number of challenges were encountered as the design process became more structured. First, the plethora of job titles within the cybersecurity industry may indicate immature role development and ambiguity. This requires an initial attempt to reduce and categorize cybersecurity titles and roles. This categorization revealed that titles would be insufficient to describe cybersecurity functions, as the titles were ambiguous within the industry itself. This required a taxonomy of functions to the be created for cybersecurity professionals outside of the use of titles. In creating this taxonomy, it became evident that organizations may poorly reflect the incorporation of cybersecurity teams into business operations, as regulatory or legal activities are poorly equipped to deal with the anomalous behavior incurred by hackers. This requires that organizations understand and prepare for a persistent threat to operations in a proportional manner to the risk that it poses. This also revealed that organizations are challenged with the cyber aspect of cybersecurity. Cybersecurity is not the manual control of computer systems to thwart attacks, but the orchestration of autonomous and manual controls to provide an appropriate level of control and security. It is both the individual and the system of systems that allow for the more efficient, or less efficient, delivery of products or services (see Table 4-1 Artifact 01 - Requirements for Cybersecurity Functions).

4.1.2 Building Artifact 01

The Taxonomy of Cybersecurity Functions

To provide a foundation for the development of the cybersecurity function taxonomy, interviews, a focus group, and professional documentation were reviewed. This provided data sets from several viewpoints that allowed for the design, build, evaluate process used to create the artifact. The following source descriptions provide details representative of the columns referenced in the appendix (see Appendix A.2 Job Titles - Thirteen Sources). Due to the variation in sources and categorization used by each source, the data was normalized within a spreadsheet and color-coded to provide additional clarity to purpose. Table 4.1 - Artifact 01 - Requirements for Cybersecurity Functions provides a concise attribution of sources used for the collection through analysis process.

Phase 1 - Collection and Aggregation

The unexpected redundancy, semantic duplication, and ambiguity required extensive data collection from several sources. Due to the paucity of resources in academic literature alone, professional and practitioner data sets were also reviewed for inclusion into the aggregate. Data sources are recorded in the appendix and referenced by source number.

Source #1 A python code was used to list all of the technology job titles (Hoyt, 2011; Zeltser & Hoyt, 2015). This figure, Figure 4-1 Cybersecurity Job Titles Analysis - Phase 1, is taken from a single site with over 7,000 titles that were codified into only 34 discrete functions.

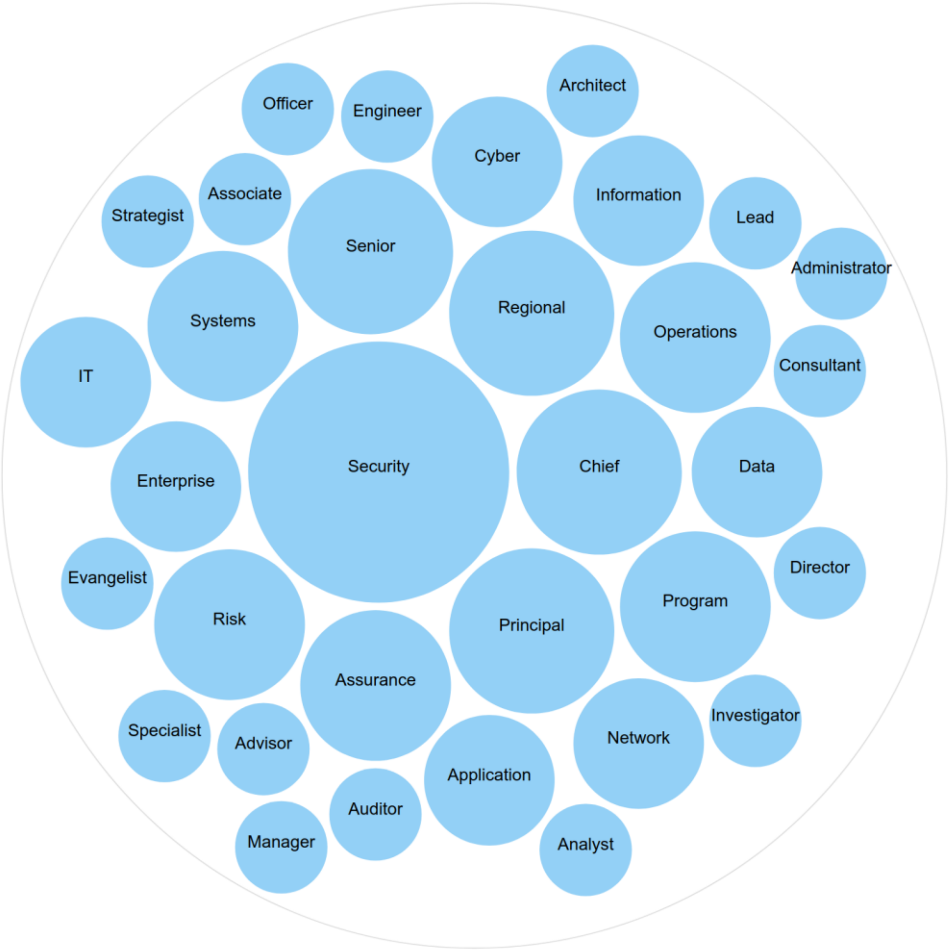
Source #2 National Institute of Standards and Technology (NIST) Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse et al., 2017)

Source #3 George Washington University (Department of Computer Science, n.d.)

Sources #4-12 Eight of the sources were cybersecurity career websites (Curran, 2016; Cyber Security Degrees and Careers, n.d.; Cybersec Jobs, n.d.; Top 10 Security Careers, n.d.; Doyle, 2019; Morgan, 2016; Rayome, 2017; Staff, 2020; Wizardry, 2018)

Source #13 INFOSEC (InfoSec Institute, 2020)

Figure 4-1 Cybersecurity Job Titles Analysis - Phase 1



Phase 2 - Normalization, Analysis, and Codification Process

In the spreadsheet, sources were listed column headings, with a unique color for each column. The job titles were listed in row headings (see Appendix A.2 Job Titles - Thirteen Sources). This allowed for the initial processing of duplicate titles to be normalized into a constructive set. The codification continued to create a taxonomy based on both the coding and initial thematic analysis (see Appendix A.4 Reduction and Codification Process). In reference to the data set within the spreadsheet, if a job title validated repeatedly in a row and marked with an "x", then that particular job title was referenced in several of the sources. For example, "Chief Information Security Officer" was identified in nine out of the thirteen sources (see Appendix A.2 Job Titles - Thirteen Sources).

Step 1: Source #1 was the largest source with 7,682 technology job titles, so the jobs from that source was listed in the first column (Zeltser & Hoyt, 2015).

Step 2: Each job title that was referenced in source #1 was marked with an "x" in that cell next to the job title in the column for that source.

Step 3: The job titles that were located in source #2 were marked with an "x" in that cell next to the job title in the column for that source.

Step 4: This process was continued for sources #3 through source #11 until all of the job titles in each source were marked on the spreadsheet.

Step 5: Any job titles that were not cross-referenced in several sources where then manually reviewed for involvement in cybersecurity. This process was completed with primarily codification; however, some outliers were thematically reduced because of undeniable replication. In cases where the job demonstrated no direct relationship to cybersecurity, for instance, "Team Lead," the job was eliminated from the inventory. This reduction reduced the data set of the total number of jobs to 2,157 (see Appendix A.4 Reduction and Codification Process).

Step 6: At this point, two previous sources (Institute, 2018; Wizardry, 2018) were reassessed as a benchmark for the comprehensive inventory, requiring additional reduction following the process in step 4. Through continued reduction, the inventory was reduced to about 200 job titles (see Appendix A.3 Job Titles Color-Coded). Note: The color of the job title cell is represented by the source that the job title was first found during the research. This was done in order from 1-13, showing all of the cybersecurity titles and colors, which references the particular source where the job title was originally discovered (see Appendix A.2 Job Titles - Thirteen Sources).

Phase 3 - Additional Data Frequency Coding and Thematic Analysis

The remaining cybersecurity titles were deconstructed into individual thematic elements. Each independent element was then processed for frequency. This was performed using several UNIX/Linux tools, including: cat, sed, awk, grep, uniq, and sort (Cowan, 2003; Irizarry, 2020). An example of a portion of this analysis is provided in the command line and output below.

This initial command shows a frequency division of title headings alone. The subsequent command shows a frequency numeration of all title terms in the original data set. The FREQ/TITLE heading is provided for ease of reading. Titles were further identified by job descriptions. Thematic analysis was used to reduce the descriptions to job functions that were representative of cybersecurity professionals. After an initial job function survey (see Appendix D.3 Job Functions Survey), respondents requested that further thematic reduction be conducted for cybersecurity positions. Jeremy Cannon (pseudonyms used) remarked, "The first three bullets in defensive can potentially be reduced to 1. (see Appendix D.3 Job Functions Survey Data)" A focus group participant, Aaron Beasley remarked,

> *Creativity and Planning and Mission Planning seem to overlap to me. I guess Mission Planning would be a big picture type of planning while Creativity and Planning would be specific solution implementations. Other than that, it looks good. I can't think of anything that is missing and the list seems pretty inclusive of functions performed by most types of cybersecurity roles. Maybe some type of Solution Research but that is probably implied with some of the already listed functions. Researching different solutions is something I feel most jobs will spend ample time doing. (D.2 Focus Group Data)*

Another focus group respondent, Ben Forton, also mentioned the need for further reduction, *"As well as what the others have said, I think that maybe External Reporting could also be an area, or merged with Internal Reporting.* (see Appendix D.2 Focus Group Data)." The Figure 4-2 Function-to-Function Visualization of Final 16 Job Categories and Table 4-2 Function-to-Function Correlation show that the resulting data set was properly correlated internally to represent cybersecurity functions. The only identified outlier is physical security which was expected as physical security is often not associated with cybersecurity roles.

Figure 4-2 Function-to-Function Visualization of Final 16 Job Categories

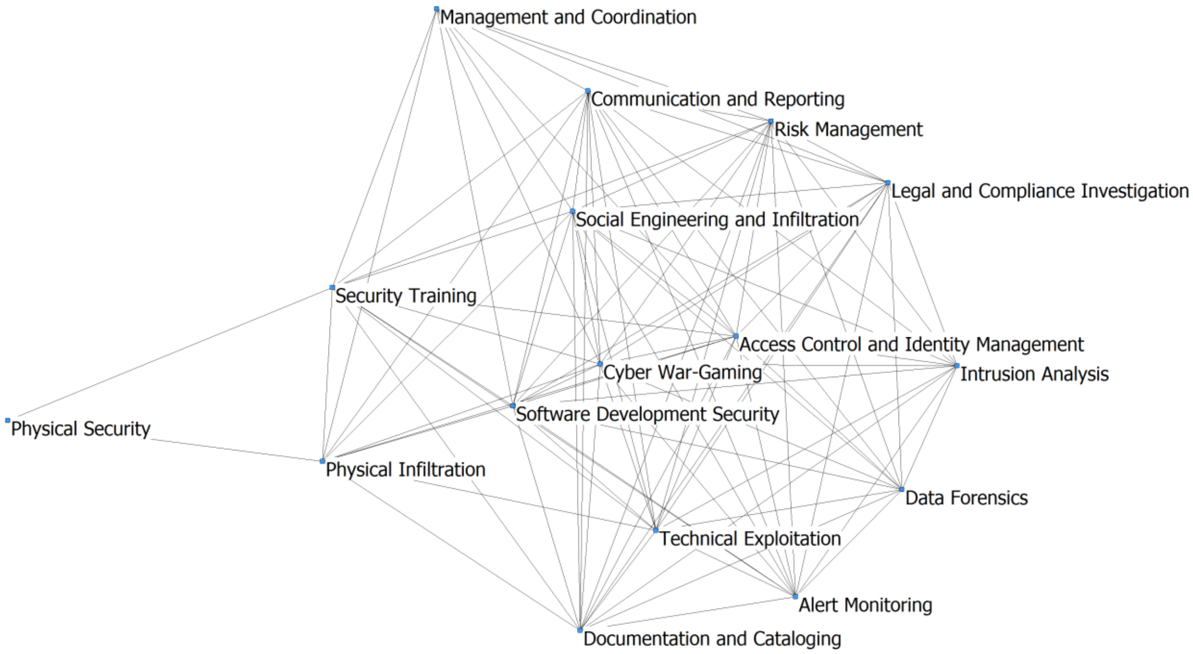

Management and Coordination
Communication and Reporting
Risk Management
Legal and Compliance Investigation
Social Engineering and Infiltration
Security Training
Access Control and Identity Management
Cyber War-Gaming
Intrusion Analysis
Software Development Security
Physical Security
Physical Infiltration
Data Forensics
Technical Exploitation
Alert Monitoring
Documentation and Cataloging

Table 4-2 Function-to-Function Correlation

Final 16 Cybersecurity Job Functions

Final 16 Cybersecurity Job Functions

Data Forensics	Access Control & Identity Management	Documentation & Cataloging	Physical Security	Intrusion Analysis	Legal & Compliance Investigation	Software Development Security	Management & Coordination	Cyber War-Gaming	Physical Infiltration	Communication & Reporting	Security Training	Risk Management	Social Engineering & Infiltration	Technical Exploitation	Alert Monitoring
1.00	0.87	0.90	−0.01	0.90	0.75	0.88	0.48	0.79	0.41	0.73	0.49	0.96	0.81	0.88	0.97
0.87	1.00	0.80	0.21	0.86	0.95	0.82	0.66	0.84	0.57	0.93	0.65	0.96	0.89	0.79	0.80
0.90	0.80	1.00	0.21	0.92	0.61	0.97	0.44	0.85	0.65	0.73	0.68	0.82	0.81	0.97	0.95
−0.01	0.21	0.21	1.00	−0.07	0.03	0.14	0.15	0.03	0.81	0.16	0.80	0.08	−0.04	0.38	0.04
0.90	0.86	0.92	−0.07	1.00	0.79	0.92	0.44	0.88	0.40	0.80	0.44	0.87	0.91	0.82	0.91
0.75	0.95	0.61	0.03	0.79	1.00	0.64	0.58	0.72	0.32	0.87	0.41	0.89	0.82	0.57	0.65
0.88	0.82	0.97	0.14	0.92	0.64	1.00	0.60	0.94	0.65	0.82	0.67	0.83	0.90	0.94	0.91
0.48	0.66	0.44	0.15	0.44	0.58	0.60	1.00	0.78	0.57	0.85	0.59	0.62	0.77	0.48	0.35
0.79	0.84	0.85	0.03	0.88	0.72	0.94	0.78	1.00	0.59	0.94	0.60	0.81	0.98	0.79	0.76
0.41	0.57	0.65	0.81	0.40	0.32	0.65	0.57	0.59	1.00	0.61	0.99	0.46	0.50	0.76	0.45
0.73	0.93	0.73	0.16	0.80	0.87	0.82	0.85	0.94	0.61	1.00	0.65	0.85	0.96	0.70	0.65
0.49	0.65	0.68	0.80	0.44	0.41	0.67	0.59	0.60	0.99	0.65	1.00	0.56	0.53	0.79	0.51
0.96	0.96	0.82	0.08	0.87	0.89	0.83	0.62	0.81	0.46	0.85	0.56	1.00	0.85	0.82	0.89
0.81	0.89	0.81	−0.04	0.91	0.82	0.90	0.77	0.98	0.50	0.96	0.53	0.85	1.00	0.74	0.76
0.88	0.79	0.97	0.38	0.82	0.57	0.94	0.48	0.79	0.76	0.70	0.79	0.82	0.74	1.00	0.92
0.97	0.80	0.95	0.04	0.91	0.65	0.91	0.35	0.76	0.45	0.65	0.51	0.89	0.76	0.92	1.00

Note. The data from the final survey are shown in this table showing that all of the cybersecurity job functions correlate correctly. The job titles are provided in the header row for a quick reference to the names of the final functions.

International Variances and Core Functions

International variation in titles was intentionally differentiated and reduced; however, this was ultimately a minor factor as the titles were reduced to a set of cybersecurity functions. An example case exhibiting such reduction would be the following: Information Systems (IS), Information Technology (IT) and Information Communications Technology (ICT) could be considered interchangeable. Through the reduction of titles to a smaller subset, it was evident that many titles were of equal description internationally or as a matter of semantics. The converse proved to be also true; some titles, for example, "cybersecurity analyst" contained descriptions that were not consistent between titles. This further supported the decision to arrive at a new core set of cybersecurity functions.

This table shows how the data collection process refined the job functions specific to the data collection title and the order in which the data was collection to showing changes in the job functions. This does not include the actual data from the respondents, as this information is included in full detail in the appendix. It does, however, include the initial and final forms for the cybersecurity functions. There is a note that the original list after initial codification was reduced to 23; however, after respondent input was received, it was found to need additional refinement to a total of 16.

Table 4-3 Job Functions Refinement

Collection Method Order	Data Collection Title	Total Job Functions	Job Functions Listed
1	Job Functions Survey	28 or 19	N/A
2	Expert Interview: Part 1	23	Alert Monitoring Creativity and Planning Cryptographic Implementation Data Forensics Disaster Recovery and Business Continuity Documentation and Cataloging Hardware Analysis Internal Reporting Intrusion Analysis Legal and Compliance Investigation Malware/Software Analysis Management and Coordination Mission Planning Physical Infiltration Public Communication Public Information Dissemination Security Training Delivery Security Training Design Service and Product Development Social Engineering and Infiltration Technical Exploitation and Penetration Testing Physical Implementation Vulnerability Communication and Disclosure
3	Expert Interview: Part 2	23	
4	Focus Group	23	

5	Cybersecurity Interest-to-Function Survey	16	Data Forensics Access Control and Identity Management Alert Monitoring Communication and Reporting Cyber War Gaming Documentation and Cataloging Intrusion Analysis Legal and Compliance Investigation Management and Coordination Physical Infiltration Physical Security Risk Management Security Training Social Engineering and Infiltration Software Development Security Technical Exploitation
6	Final Survey	16	
7	Confirmatory Interviews	16	

Note. See Appendix C.4 Expert Interview Questions - Part 1, C.4 Expert Interview Questions - Part 2, C.5 Confirmatory Interview Questions, C.6 Job Functions Survey Questions, .7. Focus Group Questions, C.8. Cybersecurity Interest-to-Function Survey Questions, C.9. Final Survey Questions

4.1.3 Design Principles – Artifact 01

A taxonomy of functions may be created for any profession through codification and thematic analysis of job titles and descriptive functions. The insufficient reduction of ambiguity, and a lack of a taxonomy of functions, complicates attempts to discretely define industry functions. In this research, 7,682 career titles were identified for cybersecurity professionals. These titles were codified and reduced to a set of sixteen discrete functions for cybersecurity professionals. Analysis indicates that occupational groupings and the development of a taxonomy are beneficial to investigation into individual performance and satisfaction (Biddle, 1986; Katz & Kahn, 1978; Nickerson et al., 2009, 2010). This is further exhibited in professional, or practitioner, cybersecurity organizations that attempt to build categories to better define their own processes and frameworks (Lewis & Rivkin, 2000; Newhouse et al., 2017; Otero, 2018; Paller, 2020). Although the data may indicate a pre-paradigmatic immaturity in the delineation of cybersecurity titles, roles, and functions, traditional factors may also affect individual satisfaction and performance. The absence of well-defined functional requirements within roles may increase the risk of a poor work environment cybersecurity staff.

Design Principle 01:

To create a taxonomy of functions for any profession, use codification and thematic analysis of job titles and descriptive functions.

Cybersecurity functions are better represented from the viewpoint of battlefield operations than that of business operations. Misrepresenting cybersecurity functions as normal business processes prevents the conceptualization that hackers are contextually out of place, invading systems outside of what is considered normal or possible. The failure to recognize the divergent characteristic of hacking within organizations and governments has led to several data leaks and other compromises (Dreibelbis et al., 2018). The actual categorization of cybersecurity functions into operational, defensive, and offensive groups as an effective strategy is already employed in the military (Department of the United States Army, 2014).

Design Principle 02:

Cybersecurity functions must be represented from the viewpoint of battlefield operations rather than that of business operations.

Cybersecurity is the symbiotic relationship between autonomous and manual controls. The misinterpretation that cybersecurity controls may be entirely enforced by a single system or individual will result in a failure to realize the system-wide complexity and involvement of human personality involved in the decision to build systems in a particular way. The inability to discern the orchestration required from both the individual and the autonomous system will result in reduced security for the organization and society. This impact in sociotechnical phenomena have become more common, allowing for greater focus on how the individual or community interacts with technology.

Design Principle 03:

To properly understand cybersecurity, it must be viewed as the symbiotic relationship between autonomous and manual controls.

4.2 Prerequisite Artifact 02 - Individual Interest Inventory

4.2.1 Artifact 02 - Requirements for an Individual Interest Inventory

Table 4-4 Artifact 02 - Requirements for an Individual Interest Inventory

Design Challenges	**Artifact Requirements**	**Justificatory Knowledge (Academic/Practitioner)**	
		Theory	**Authors**
	AR05: Individual Interests must be defined in the constrains of the cybersecurity profession.	Agency Theory	(Jensen & Meckling, 1976; Mitnick, 1976)
DC05: Individual interests and psychometrics may be too broad for relevant application to a career or industry.		Five Factor Model (FFM)	(Digman, 1990)
		Gati's Model	(Gati et al., 1996)
	AR06: Interest categories must be created and reduced to a discrete and distinguishable subset.	Holland Vocational Interest Inventory (RIASEC)	(Holland, 1986)
		Job Characteristics Model	(Hackman & Oldham, 1976)
		Jung Typology	(Jung, 1921)
DC06: Cybersecurity professionals are sometimes seen as a homogeneous group, sharing common interests, desires, and goals.		Met Expectations	(Porter & Steers, 1973)
	AR07: Discrete interests possessed by each individual should be defined and made distinguishable by industry professionals.	Self-Determination	(Deci & Ryan, 2008)
		Taxonomy of Vocational Interests	(Jackson et al., 1984)
		Unfolding Model	(Lee & Mitchell, 1994)
		Withdrawal Model	(Hulin, 1991)

During the design process for the second prerequisite artifact, two primary challenges were encountered: 1) Individual interests and psychometrics may be too broad for relevant application to a career or industry and 2) Cybersecurity professionals are sometimes seen as a homogeneous group, sharing common interests, desires, and goals. Although this area of research was far more mature than what was available for the first artifact, the initial challenge required a thorough investigation into a representative set of psychometric profiling solutions. This resulted in a requirement that the individual interests for cybersecurity employees must be related to the functions within cybersecurity, not broad psychological measurements. In order to define individual interests outside of psychometric functions, a new set of interests much be determined and reduced to a discrete and distinguishable subset. Finally, because cybersecurity professionals were seen to possess monolithic, or common, interests, discrete interests possessed by each individual must be defined and made distinguishable by industry professionals (see Table 4-4 Artifact 02 - Requirements for an Individual Interest Inventory).

4.2.2 Building Artifact 02

Phase 1 - Collection and Aggregation

To accomplish the logical integration of individual interests into a final inventory, it was first necessary to delineate how traits were defined for established interest or profiling solutions. To accomplish this task, psychometric and practitioner literature was reviewed, codified, and thematically analyzed into a categorical system. From a psychometric perspective, the Five Factor Model, Jung Typology, and Holland's Codes were selected as representative models and individually indexed, then aligned to remove any duplication of measurements from each profile, and then reintegrated into a single tuple of personality measurement. The functions from the first artifact were used as guidelines for the determination of relevant interest traits. This created a relation instance that could be associated with each cybersecurity function attribute defined into a matrix. This matrix can then be used to assign a binary indicator to each attribute value as it applies to both the individual interest and functional attribute. This process offered far less ambiguity and greater alignment potential than the determination of cybersecurity functions in the first artifact.

The initial codification began with the Five Factor Model (FFM). The FFM is unable to attribute specific psychological traits to specific job functions, as this is out of the scope of the test itself; however, this may not eliminate the test from successful personality-to-function analysis in future research. This places the FFM on the broad end of the spectrum of personality-to-function psychometrics, allowing organizations an additional tool in the proper allocation of individuals to broader aspects of organizational culture. Next, The Jung Typology was analyzed for determination of individual interests. The Jung Topology naturally presented itself as an examination of how individuals process situational information (Wilk & Sackett, 1996). This possibly indicated that the Jungian traits would be well suited in terms of management style as opposed to career function. Finally, the Holland's Codes or RIASEC model was considered as a representative psychological guideline for the determination of individual interest codes. The RIASEC model has been integrated into many career tests around the world in different languages because it is easy to understand, the VPI and SDS tests are widely accessible, and it links occupation codes from a variety of sources to the Holland Codes (McDaniel & Snell, 1999). Holland's approach of using empirical data to determine personality-to-function metrics allows for the extrapolation of personality type to a multitude of job functions. This specificity allows for some respective functions to be associated to an individual's personality profile. Currently, the U.S. Department of Labor has sponsored O*NET, the Open Source Psychometrics Project designed for career counseling using the RIASEC constructs (Lewis & Rivkin, 2000). A test called the O*Net Interest Profile is available to anyone online and then detailed job descriptions are given based on their RIASEC codes (Lewis & Rivkin, 1999; Rounds & Walker, 1999).

An additional comment by an expert interviewee, Michael Brown, provided further clarify the categories in an expert interview, *"I'm not sure if it was just me or the "Research and Investigation" category is too broad* (see Appendix C.4 Expert Interview Questions - Part 1 and D.1 Expert Interview 1 Data). To give further credence to the interests, out of the 6 individual preferences listed, none of the expert interviewees selected any to be removed from the list, and nothing was suggested to be added to the list (see Appendix C.4 Expert Interview Questions - Part 2). Also, in the focus group, James Hampton explained his opinion that the interest categories would sufficiently represent various factors important to individual satisfaction and stated: *"These seem reasonable to me* (see Appendix D.2 Focus Group Data)." In the Cybersecurity Interest-to-Function Survey, several relationships between the job functions and individual interests were seen in the data results. For example, leadership and vision is an individual trait that four participants felt is important for management and coordination, and three participants chose sociable and diplomatic skills as important for communication and reporting and security training job functions (see Appendix D.4 Cybersecurity Interest-to-Function Survey Data).

Unfortunately, after introduction research was complete, the alignment between psychometric profiles and specific cybersecurity careers was too limited to pursue. Although there is some relationship between the different psychometric profiles of the FFM, Jung, and RIASEC, this was only a significant marker of employee performance and individual satisfaction when all three were codified, reduced, and a thematic application to specific cybersecurity roles was applied. This required the creation of a non-psychometric inventory of individual preferences that were respective to cybersecurity functions. This new interest inventory provided a more accurate assessment of the cybersecurity employee's interest-to-function alignment. Each of the psychometric profiles has been associated with traits found in cybersecurity functions in the variable associate matrix (Tokar et al., 1995).

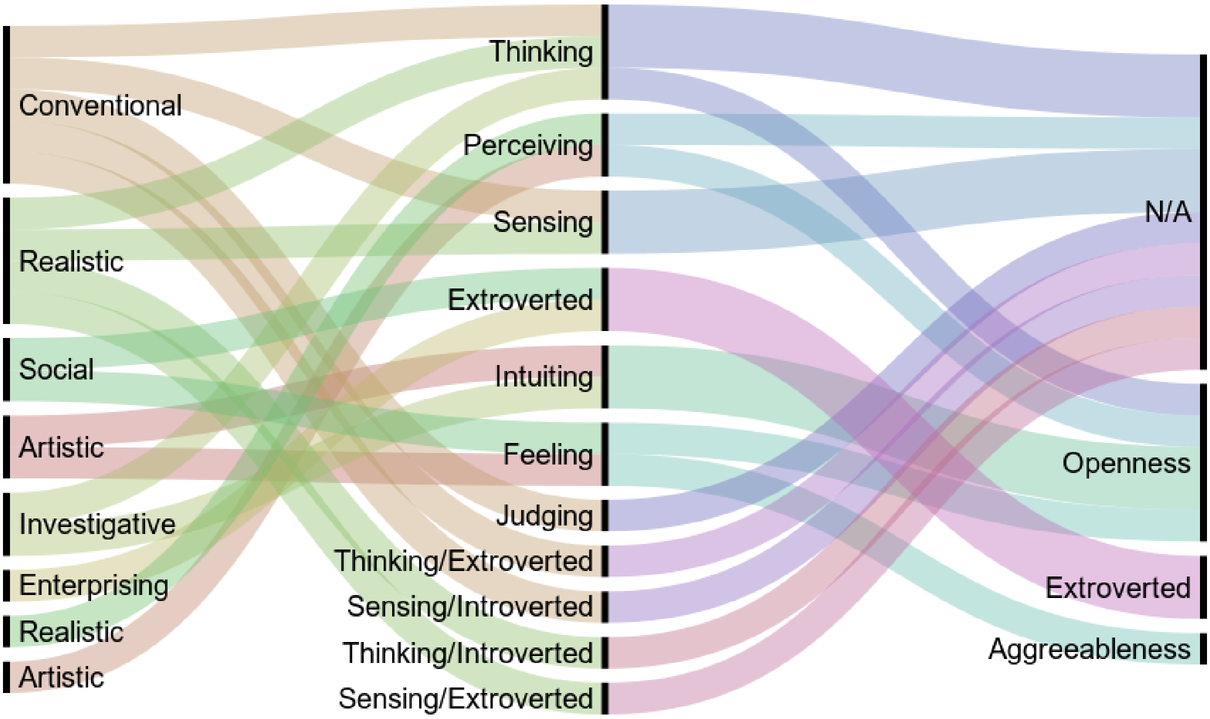
Phase 2 - Codification and Thematic Analysis

Initially, alignment exercises were conducted on the Five Factor Model. The primary traits of concern within the BIG 5 are Conscientiousness, Agreeableness, and Neuroticism. These traits do not assist in the suitability for a specific cybersecurity role; however, they provide basic traits that are common for performance and individual satisfaction. Individuals who score high in "Conscientiousness" are more likely to feel obligated to get their job done. Those who score high in "Agreeableness" are more likely to get along with other staff members and management. Those who score high in "Neuroticism" are more likely to be unsatisfied and argumentative.

Next, the Jung Typology was evaluated against cybersecurity functions. This model provides traits that are more specific to corporate culture, office dynamics, and management style. The primary areas of concern are: (I)Individual vs. (E)Group, (N)Ambiguity vs. (S)Structure, and (F)Feelings vs. (T)Facts. Unlike the FFM, this analysis does not provide an obvious selection for improved performance or individual satisfaction. This is due to the requisite alignment of the personality trait to the character of the organization. An organization that needs a highly active team player would need to avoid an excessively introverted candidate. If a large amount of structure is provided within the job, individuals who value freedom and ambiguity would be a poor fit. If the position works with customers or fellow employees in a support or management role, an individual who communicates with feeling would be a better option.

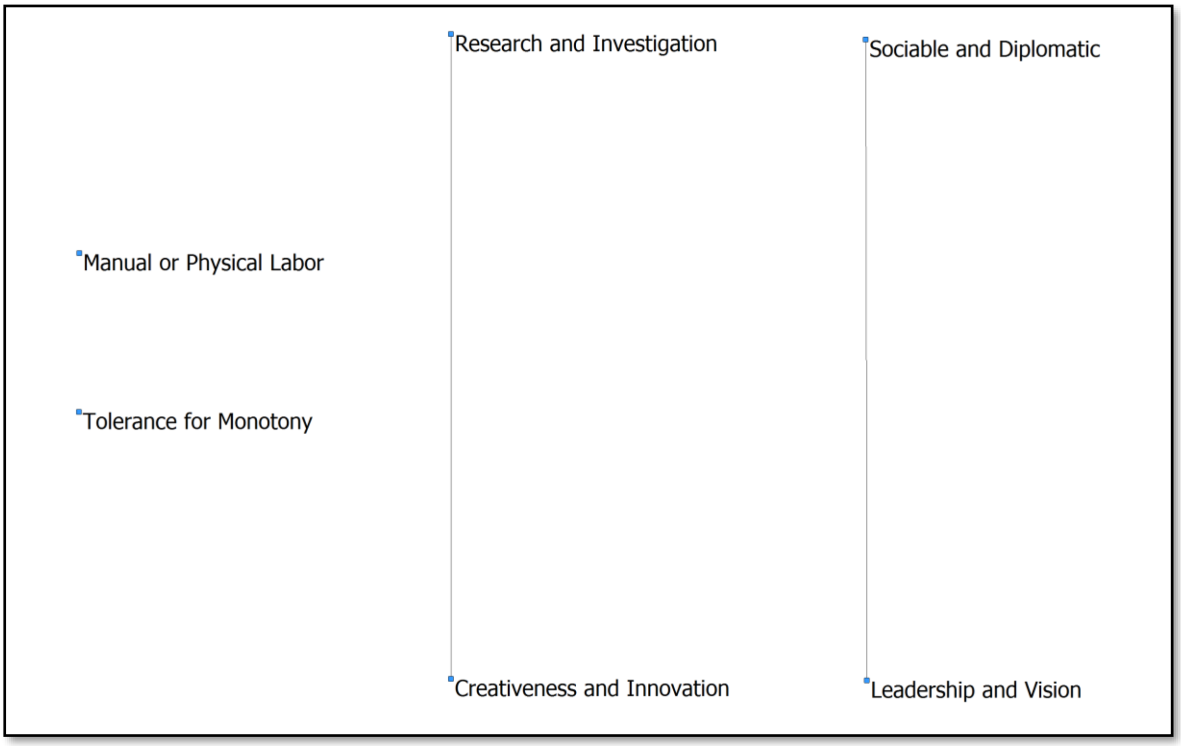
Finally, an alignment was conducted between RIASEC and cybersecurity functions. This model provides traits that will directly be aligned with the individual's vocation. Concerns about neuroticism, teamwork, or other factors covered in the previous psychometrics are not evaluated. In this case, the ability to work on concrete items, investigate potential solutions, provide creative ideas, help others, see new opportunities, or work on monotonous projects is evaluated (see Figure 4-3 Psychometric Alignment).

Figure 4-3 Psychometric Alignment



The evaluation of portions of formal psychometrics and career interest topics allows for the creation of an Individual Interest Inventory. This can be used as a survey tool for prospective cybersecurity career seekers, allowing the alignment of individual interests to cybersecurity functions below. This analysis was further conducted using a semantic engine. This took the traits identified in each of the psychometric profiling solutions and provided a visual representation of the alignment. These factors were further codified to cybersecurity functions resulting in the Individual Interest Inventory (III). The new preference factors developed are centered on an individual's desire for the following type of work: Implementation, Investigation, Creative, Social, Organizational, and Leadership. The figure and corresponding table illustrate that there was adequate differentiation between the individual interests selected within the research (see Figure 4-4 Visualization of Final Six Categories and Table 4-5 Interest-to-Interest Correlation). These interests were originally composed of thirty-six different traits that were reduced through focus group and interview meetings to a discrete set of six. The absence of interconnected lines visualizes the lack of excessive correlation between the data points. The four aspects that do maintain a small degree of correlation were expected, as research does require a significant level of creativity, and leadership does require a significant level of socialization. Even so, both of these correlations are discernible individually. Interest-to-Interest.

Figure 4-4 Visualization of Final Six Interest Categories



Note. This visualization shows that there was adequate differentiation between the final 6 categories of individual interests selected within the research. The vertical lines are links representing the internal correlation of the terms.

Table 4-5 Interest-to-Interest Correlation

	Manual or Physical Labor	Research and Investigation	Creativeness and Innovation	Sociable and Diplomatic	Leadership and Vision	Tolerance for Monotony
Manual or Physical Labor	1.000	-0.609	-0.563	-0.184	-0.187	0.065
Research and Investigation	-0.609	1.000	0.397	-0.338	-0.025	0.010
Creativeness and Innovation	-0.563	0.397	1.000	-0.219	-0.205	-0.405
Sociable and Diplomatic	-0.184	-0.338	-0.219	1.000	0.291	-0.205
Leadership and Vision	-0.187	-0.025	-0.205	0.291	1.000	-0.119
Tolerance for Monotony	0.065	0.010	-0.405	-0.205	-0.119	1.000

Note. The data for the final survey are shown in this table showing that all of the individual interests correlate correctly. The six individual interests are listed on the header rows for a quick reference.

4.2.3 Design Principles – Artifact 02

Individual interest inventories may be created for any profession through codification and surveys that align the respective industry functions to individual behaviors that are beneficial to those functions. Without the use of individual input from career-specific segments of society, it is not possible to delineate the behaviors that are beneficial to the respective function. The analysis shows that the expert respondents favored a reduction to easily discernible interest groups. They also provided input concerning the ambiguity that they believe existed between some terms and cybersecurity functions as a whole. One respondent remarked, "*I'm not sure if it was just me or the "Research and Investigation" category is too broad. I feel like for almost anything IT or cybersecurity related I would find myself researching online whatever I'm working on."* This relatively small remark revealed the inadequacy of using psychometric testing as a single tool. In this case, a psychometric response of "intuitive" would need to be thematically adjusted to conform to an actual cybersecurity function (Joseph et al., 2012). The resulting work provided a clear list of interests that did not exhibit positive correlation to one another.

Design Principle 04:

To properly align industry functions to individual interests, create specialized individual interest inventories that are specific to that industry.

Cybersecurity professionals are not represented by a monolithic category of interests; conversely, their interests vary widely in the types of work they prefer to perform. The inference that cybersecurity professionals all maintain a similar or monolithic set of interests invalidates attempts to properly define both organizational team dynamics and individual functions. As stated in the expert interviews, individuals vary widely in the types of tasks that they enjoy. This variance in interest and desired tasking further supports that individuals within cybersecurity should be seen as individual persons, each with their own goals and desires that are beyond the common interests of their peers. Furthermore, the selection of six interest categories by interview, focus group, and survey, demonstrated the variation of interests that individual cybersecurity professionals wanted to see represented in this research.

Design Principle 05:

Avoid monolithic collectivism of interests for cybersecurity professionals, their interests vary widely in the types of work they prefer to perform.

4.3 Integrated Artifact 03 - Interest-to-Function Alignment

4.3.1 Artifact 03 - Requirements to Align Individual Interests to Cybersecurity Functions

Table 4-6 Artifact 03 - Requirements to Align Individual Interests to Cybersecurity Functions

Design Challenges	**Artifact Requirements**	**Justificatory Knowledge (Academic/Practitioner)**	
		Theory	**Authors**
DC07: Individual interests are sometimes misaligned to the tasks within a role, resulting in less productivity, retention, and satisfaction.	**AR08**: A system to align individual interests with cybersecurity functions must be developed.	Intermediate Linkage Model	(Mobley, 1977)
		IT Career Paths	(Joseph et al., 2012)
		IT Turnover Theory	(Joseph et al., 2007)
	AR09: The artifact must be evaluated as the primary output of the design science process.	Job Embeddedness Theory	(Mitchell & Lee, 2001)
DC08: On occasion, the design and manufacture of an artifact may be undertaken without fully understanding the challenge.		Personality Dimensions	(Judge et al., 1999)
	AR10: Careful attention must be applied to the scientific method and knowledge.	Theory of Organizational Equilibrium	(March & Simon, 1958)
		Turnover Model	(Steers and Mowday, 1981)
		Person-Environment Fit Theory	(Edwards et al., 1998)

The design of the integrated artifact 03 presented a set of challenges for role alignment to organizational function and individual interests. Specifically, individual interests are sometimes misaligned to the tasks within a role, resulting in less productivity, retention, and satisfaction. A system to align individual interests with cybersecurity functions must be developed. Next, a general concept that involves design science arose that is unique. On occasion, the design and manufacture of an artifact may be undertaken without fully understanding the challenge. Care must be taken that the artifact must be evaluated as the primary output of the design science process and careful attention must be applied to the scientific method and knowledge contribution throughout the process (see Table 4-6 Artifact 03 - Requirements to Align Individual Interests to Cybersecurity Functions).

4.3.2 Building Artifact 03

The integrated artifact, Artifact 03, aligns the interest inventory and functional cybersecurity aspects into a single prescriptive model.

Conceptual Model

1. The combination and reduction of the FFM, MBTI®, and RIASEC psychometric profiles into the Individual Interest Inventory provides tools from which the individual's personality can be aligned with the tasks or roles to impact individual satisfaction. This results in higher satisfaction in a range from 20% to 70% for the individual employee as indicated in Rothstein and Goffin’s research : "20% (Geller, 2004), 30% (Berta, 2005), 40% (Daniel, 2005), and even 70% (Wagner, 2000) (Rothstein & Goffin, 2006)."
2. Workplace and Job satisfaction will impact the employee's intention to retain their employment (Mobley, 1977).
3. The proper alignment of an individual's personality-to-position will also cause an improvement in performance (Edwards et al., 1998; Tett & Jackson, 1991).

In order to potentially derive an alignment between job function and individual personality in the field of cybersecurity, all functional requirements for cybersecurity employees were reduced to three broad categories: Operational Functions, Defensive Functions, and Offensive Functions. As a subset of each of these broad categories, cybersecurity workloads were recorded into each respective group. Cybersecurity functions are different than many normative business operations, but they do possess analogs in other industries and functional departments.

The variables are defined in terms of psychometric profiles for each individual employee. This is, by proposed necessity, a combination and conversion of the Five Factor Model (FFM), the Jung Typology (Jung/MBTI®), and the Holland Codes (RIASEC) to the Individual Interest Inventory. The percentage of an employee's match to each of the personality traits in the profiles and job functions should provide a determination of the individual's potential satisfaction. This will be analyzed through a combination of interest inventories and a functional characteristics survey.

Each personality aspect is calculated on what is believed to be the most significant traits for each cybersecurity position. This alignment is listed in Table 4-7 Final Artifact Categories.

Table 4-7 Final Artifact Categories

Artifact 01	**Artifact 02**
Final Sixteen Cybersecurity Job Function Categories	**Final Six Individual Interests Categories**
Data Forensics	
Access Control and Identity Management	
Documentation and Cataloging	
Physical Security	
Intrusion Analysis	
Legal and Compliance Investigation	Manual or Physical Labor
Software Development Security	Research and Investigation
Management and Coordination	Creativeness and Innovation
Cyber War-Gaming	Sociable and Diplomatic
Physical Infiltration	Leadership and Vision
Communication and Reporting	Tolerance for Monotony
Security Training	
Risk Management	
Social Engineering and Infiltration	
Technical Exploitation	
Alert Monitoring	

The sections below describe the process for the final artifact. This allows for the reconstruction of the research that was conducted using interest-to-function correlative data points. As referenced earlier, there is no set of humanly discernible data points that can encapsulate every individual interest or every task a person may be required to perform. These data points allow for a measurable correlation between simplified interests and functions that are representative of the whole of cybersecurity functions. In this case, both cybersecurity functions and individual interests were categorized into a representative taxonomy in the prerequisite artifacts Table 4-7 Final Artifact Categories.

Once the data from the first two artifacts was analyzed, two additional processes were used to normalize the data. First, the data from the survey are organized into columnar sets and averaged, reducing the total survey results to percentages respective to each interest and function. Next, the data are place into tab-separated and comma-separated matrices. This allows the data to be imported into link analysis software and processed from the Linux command line. The normalization process is described in the following paragraphs. Extensive use of UNIX/Linux was incorporated to process the datasets. These tools are well-known for their data processing capabilities and unrivaled abilities to quickly and correctly process text (Cowan, 2003; Irizarry, 2020). Bash was the primary shell, allowing the use of all of the functions, variables, loops, and scripting capabilities to quickly evaluated the aggregated data.

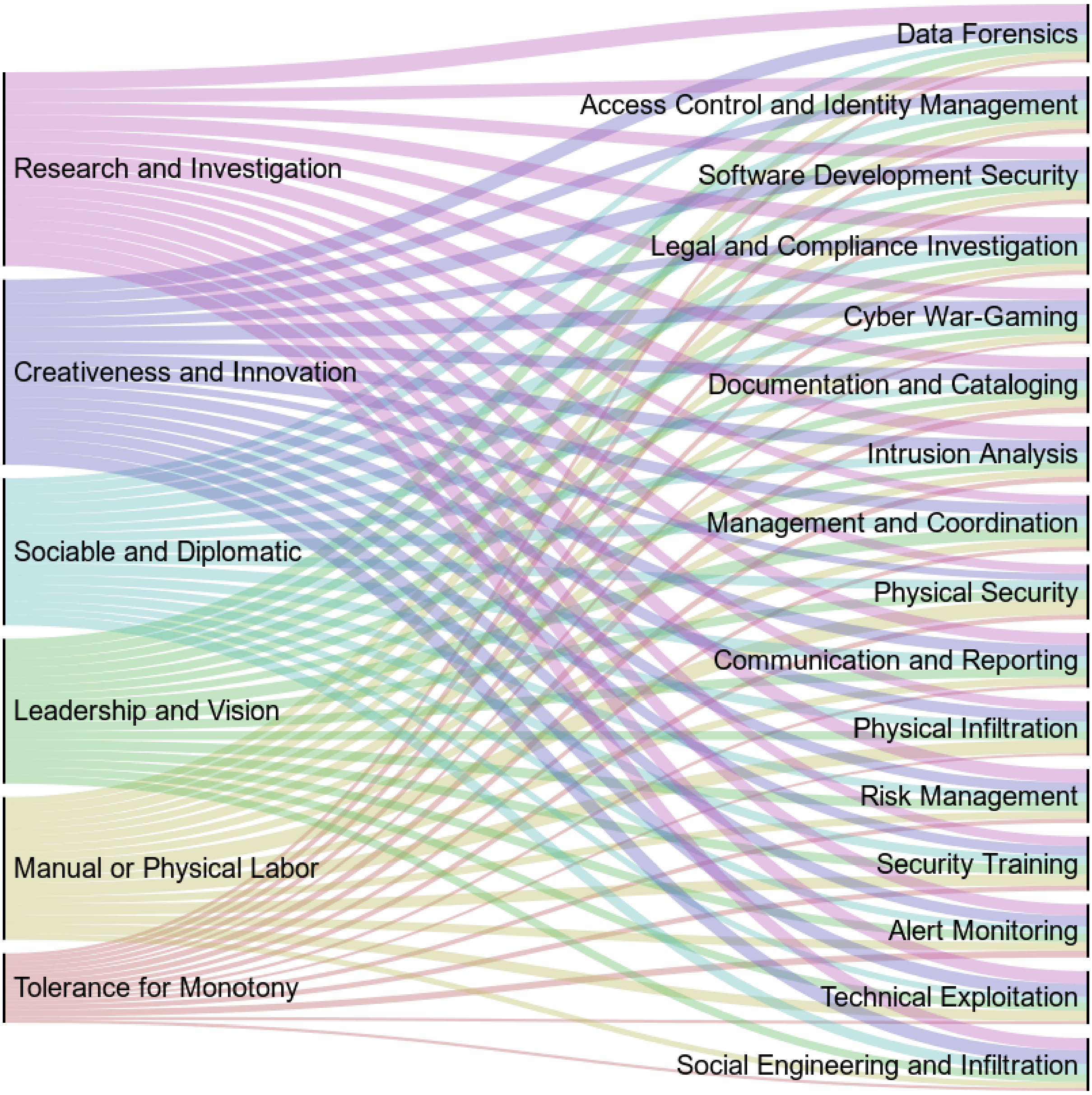
A visualization engine called, "RAWGraphs" was used to output visual representations. This method is very useful in the processing of textual analysis taken from the command line for processing into human-readable output. The ability to output visual representations of data is important to the quick assimilation of data meaning. This data analysis was accomplished through several successive attempts to best represent the data interest-to-function alignment. These attempts were conducted through several permuted iterations of the bash code in Figure 4-5 Bash Code Example.

Figure 4-5 Bash Code Example

```
IFS=$'\n'; echo -e "Function\tIntensity\tInterest"; for var_list in `cat read.categories`; do
var_title=`cat sort.$var_list | head -1 | cut -c 9- `; for line in `cat sort.$var_list | tail -6`; do
printf "$var_title\t$line\n"; done ; done | sort | sed -r 's/[0-9][0-9]+/&\t/'
```

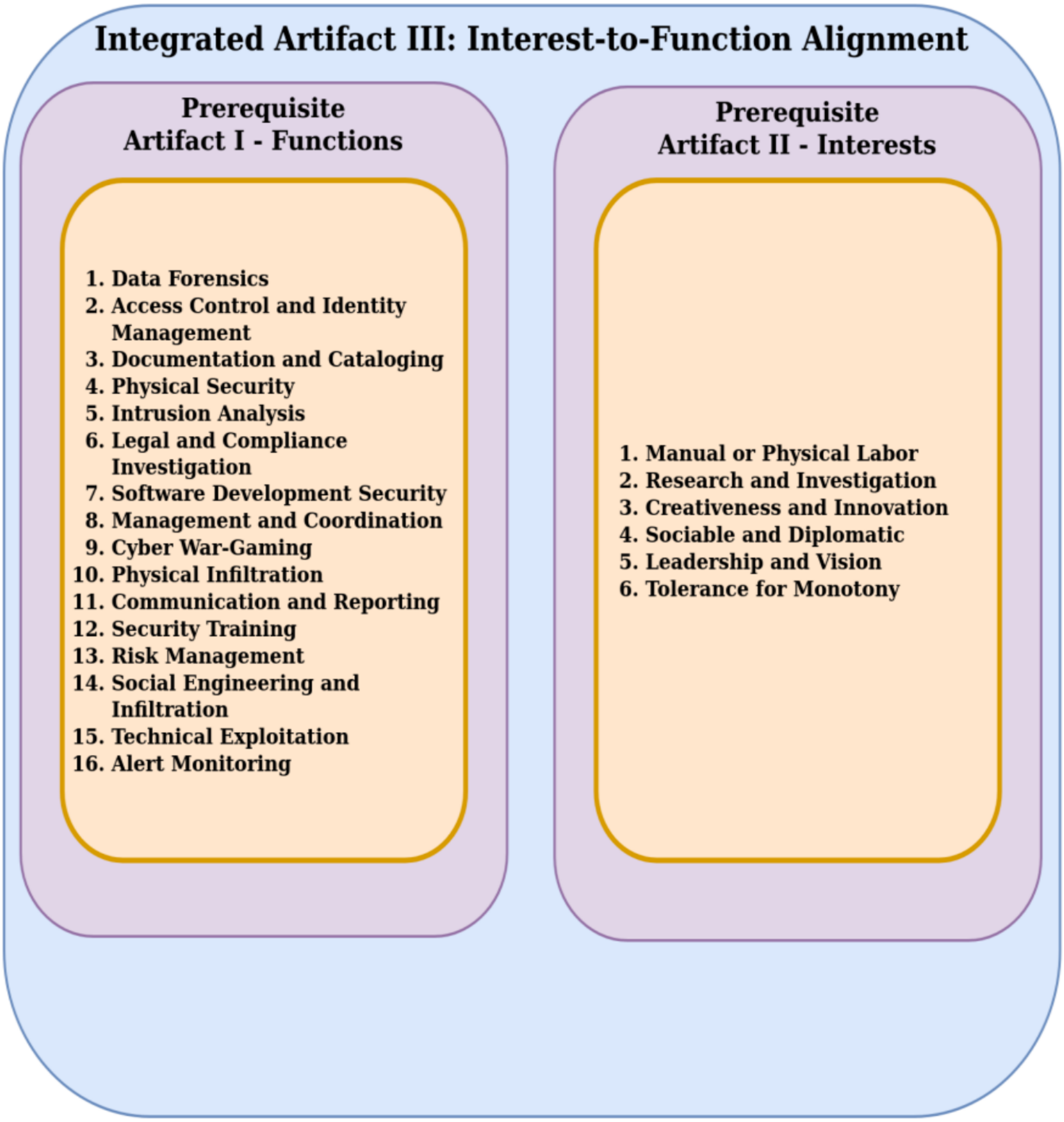
After arriving at a text-based analysis that provided the needed data points, RAWGraphs was used to visualize the data Figure 4-6 Interest-to-Function Data Visualization.

Figure 4-6 Interest-to-Function Data Visualization



This alluvial visualization provided an interest-to-function graph that illuminated the relationships that are shared between each category. These relationships become more defined throughout the process. An alluvial visualization was used to allow for easy identification of intensity and of associations. In this graphic, the six individual interests are listed in order based on the data received. The most common trait for all functions within cybersecurity careers is research and investigation, followed by creativeness and innovation. The least identifiable interest for cybersecurity professionals is a Tolerance for Monotony (TfM). An individual with a high degree of tolerance for monotonous and repetitious work is best suited for data entry-type positions that do not require engaging complex system interactions or potential threats. These results were in line with the expectations concerning cybersecurity interest-to-function relationships. The prerequisite artifacts can be seen as part of the integrated artifact in both Figure 4-7 Integrated Artifact 03 and Appendix A.1 Artifact 03 Cybersecurity Interest-to-Function Alignment Model.

Figure 4-7 Integrated Artifact 03



Integrated Artifact III: Interest-to-Function Alignment

Prerequisite
Artifact I - Functions

1. Data Forensics
2. Access Control and Identity Management
3. Documentation and Cataloging
4. Physical Security
5. Intrusion Analysis
6. Legal and Compliance Investigation
7. Software Development Security
8. Management and Coordination
9. Cyber War-Gaming
10. Physical Infiltration
11. Communication and Reporting
12. Security Training
13. Risk Management
14. Social Engineering and Infiltration
15. Technical Exploitation
16. Alert Monitoring

Prerequisite
Artifact II - Interests

1. Manual or Physical Labor
2. Research and Investigation
3. Creativeness and Innovation
4. Sociable and Diplomatic
5. Leadership and Vision
6. Tolerance for Monotony

4.3.3 Design Principles – Artifact 03

The proper alignment of individual interests to cybersecurity functions may result in increased individual satisfaction and performance. The improper alignment of an individual's personal interests will result in dissatisfaction and a loss of performance. The expert interviewees commented that the ability to properly align their employees to cybersecurity tasks within their organizations would be highly desirable. This was further developed in one interview where the cybersecurity business owner stated that organizations would be able to redesign their cybersecurity departments to better fit with the concepts discussed in the employee interest and function tables. The need to better provide aligned tasks for their staff was repeated by two business owners from two global hemispheres without recommendation within the interview. This further underscores the challenge that medium and large business owners face in providing for their cybersecurity staff.

Design Principle 06:

To achieve increased individual satisfaction and performance, properly align individual interests to cybersecurity functions.

In Design Science, identifying and expressing the question or challenge that needs to be overcome concisely and with precision should be the primary focus. Only through proper identification of the problem, can one hope to provide an adequate solution. Hevner, Peffers, Gregor, Vaishnavi, Kuechler, Simon, Fuller, Thuan, and Thakurta are especially helpful in providing standards and analysis for the development of design science research. These guidelines require that the researcher understands the problem thoroughly, if not at the beginning of the process, by the evaluation of the artifact that was created. It may be true that scientists may not truly understand their challenges upon the onset of their research; however, care must be taken to avoid being swept away in the process of investigation and research. Design science researchers cannot contribute only a new method or viewpoint to the community, they must contribute a solution in an artifact or several artifacts. This may require the repeated research into topics that were originally considered tangential at the beginning of the research, that later became foundational. This requirement to produce an artifact, under scientific rigor, that expands the body of scientific knowledge remains the driving force behind design science research, and the proper identification of the final solution, in an artifact, must be the primary goal.

Design Principle 07:

To develop an artifact within Design Science, the primary focus is to understand and address the challenge.

4.4 Summary

Although additional processes may be included, the identification of a challenge in abstract terms, followed by the respective development of an abstract solution, which results in a real instantiation of an artifact should inherently provide the steps needed to complete a cycle of a design principle in use. This may be considered possible because the artifact itself will require a design, build, and evaluation cycle that further refines the entire process internally. This is a modification of Gregor's work, as represented here: [abstract problem]==>[abstract solution]==>[artifact/real solution] (Gregor et al., 2020).

The final tables below Table 4-8 Design Principle Literature and Data Justification and Table 4-9 Design Principles Summary with Corresponding Artifact, Challenge, and Requirement represent the artifacts, challenges, principles, and source information used for each. This provides additional resource for the reconstruction of the research to provide additional research opportunities.

Table 4-8 Design Principle Literature and Data Justification

	Artifact 01			Artifact 02		Artifact 03	
	DP01[1]	**DP02**	**DP03**	**DP04**	**DP05**	**DP06**	**DP07**
Literature	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expert Interview: Part 1	Yes	Yes	Yes	Yes	Yes	--	--
Expert Interview: Part 2	Yes	Yes	Yes	Yes	Yes	--	--
Confirmatory Interview	--	--	--	--	--	Yes	Yes
Focus Group	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Job Functions Survey	Yes	Yes	Yes	--	--	--	--
Cybersecurity Interest-to-Function Survey	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Final Survey	Yes	Yes	Yes	Yes	Yes	Yes	Yes

[1] Design Principle (DP) Number

Note. This table shows the relationship of how the seven design principles correspond to each of the three artifacts, the eight design challenges and the ten artifact requirement in this study.

Table 4-9 Design Principles Summary with Corresponding Artifact, Challenge, and Requirement

	Design Principle	Artifact	Design Challenge	Artifact Requirement
DP01[1]	To create a taxonomy of functions for any profession, use codification and thematic analysis of job titles and descriptive functions.	Artifact 01	DC01 DC02 DC03 DC04	AR01 AR02 AR03 AR04
DP02	Cybersecurity functions must be represented from the viewpoint of battlefield operations rather than that of business operations.			
DP03	To properly understand cybersecurity, it must be viewed as the symbiotic relationship between autonomous and manual controls.			
DP04	To properly align industry functions to individual interests, create specialized individual interest inventories that are specific to that industry.	Artifact 02	DC05 DC06	AR05 AR06 AR07
DP05	Avoid monolithic collectivism of interests for cybersecurity professionals, their interests vary widely in the types of work they prefer to perform.			
DP06	To achieve increased individual satisfaction and performance, properly align individual interests to cybersecurity functions.	Artifact 03	DC07 DC08	AR08 AR09 AR10
DP07	To develop an artifact within Design Science, the primary focus is to understand and address the challenge.			

[1] Design Principle (DP) Number

5 Conclusion and Evaluation of Research

5.1 Introduction

This chapter concludes the research investigation undertaken to create an interest-to-function alignment model for cybersecurity professionals. The research questions, contribution to knowledge, implications, and limitations are stated below to assist in additional research that may be seen as constructive in addressing the challenges stated within this study. It is hopeful that this research will be useful for both the critical and innovative generation of additional solutions to address the many challenges of cybersecurity employment, structure, retention, performance, and satisfaction involving every industry and cybersecurity professional around the world.

5.2 Addressing the Research Questions and Propositions

The purpose of this research was to investigate the need within organizations to acquire additional cybersecurity professionals, or to retain existing cybersecurity professionals, in the face of persistent and growing international threats (Crumpler & Lewis, 2019). In order to accomplish this task, individual satisfaction and performance were analyzed across individual interests and organizational cybersecurity functions. It was determined that creating a model that aligned individual interests with cybersecurity functions would provide value for both performance and satisfaction for the individual and the organization (Aruna & Anitha, 2015; Park & Shaw, 2013). The analysis of individual satisfaction as a factor for employment intention or retention, as well as a factor for improved performance was established through existing models and literature (Oltsik, 2019). The primary challenges to the research developed when attempting to determine cybersecurity job functions and individual interests that apply to the aforementioned cybersecurity functions. This led to the development of three propositions and artifacts that would require several permutations of design and evaluation to finally achieve a model that could solve the alignment challenge (see Table 5-1 Propositions Aligned to Artifacts). The development of these artifacts also rendered additional contributions to cybersecurity organizational design and career challenges (see Table 5-2 Research Problem, Questions, Propositions, Artifacts, and Design Principles Details).

Table 5-1 Propositions Aligned to Artifacts

Proposition	Artifact
Proposition 01: Taxonomy of Job Functions Therefore, this research proposes the development of a taxonomy of cybersecurity functions for use in a new model that will align to individual interests.	**Artifact 01** Taxonomy of Job Functions
Proposition 02: Taxonomy of Interests Therefore, this research proposes the development of a specific taxonomy of interests that would align directly with the cybersecurity profession	**Artifact 02** Taxonomy of Interests
Proposition 03: Alignment of Interests to Functions Therefore, this research proposes the combination of the taxonomy of functions and the taxonomy of interests to create an aligned relationship between the two.	**Artifact 03** Alignment of Interests to Functions

Table 5-2 Research Problem, Questions, Propositions, Artifacts, and Design Principles Details

<table>
<tr><td colspan="7">Research Problem:
There is a Shortage of Cybersecurity Professionals Worldwide</td></tr>
<tr><td colspan="7">⬇</td></tr>
<tr><td colspan="7">RQ
It what ways would it be possible to improve acquisition and retention of cybersecurity professionals?</td></tr>
<tr><td colspan="3">⬇</td><td colspan="4">⬇</td></tr>
<tr><td colspan="3">RSQ
What prevents proper acquisition of Cybersecurity Professionals?</td><td colspan="4">RSQ
What prevents proper retention of Cybersecurity Professionals?</td></tr>
<tr><td colspan="3">⬇</td><td colspan="2">⬇</td><td colspan="2">⬇</td></tr>
<tr><td colspan="3">RQ
How can cybersecurity functions be better defined?</td><td colspan="2">RQ
How can the individual interests of cybersecurity professionals be better considered?</td><td colspan="2">RSQ
What factors should be required in the design of an interest to function career alignment model?</td></tr>
<tr><td colspan="3">⬇</td><td colspan="2">⬇</td><td colspan="2">⬇</td></tr>
<tr><td colspan="3">P01
Proposition 01: Taxonomy of Job Functions

Therefore, this research proposes the development of a taxonomy of cybersecurity functions for use in a new model that will align to individual interests.</td><td colspan="2">P02
Proposition 02: Taxonomy of Interests

Therefore, this research proposes the development of a specific taxonomy of interests that would align directly with the cybersecurity profession.</td><td colspan="2">P03
Proposition 03: Alignment of Interests to Functions

Therefore, this research proposes the combination of the taxonomy of functions and the taxonomy of interests to create an aligned relationship between the two.</td></tr>
<tr><td colspan="3">⬇</td><td colspan="2">⬇</td><td colspan="2">⬇</td></tr>
<tr><td colspan="3">A01
Cybersecurity Career Functions</td><td colspan="2">A02
Individual Interest Inventory</td><td colspan="2">A03
Interest-to-Function Alignment</td></tr>
<tr><td>⬇</td><td>⬇</td><td>⬇</td><td>⬇</td><td>⬇</td><td>⬇</td><td>⬇</td></tr>
<tr><td>DP01
Design Principle 01:

To create a taxonomy of functions for any profession, use codification and thematic analysis of job titles and descriptive functions.</td><td>DP02
Design Principle 02:

Cybersecurity functions must be represented from the viewpoint of battlefield operations rather than that of business operations.</td><td>DP03
Design Principle 03:

To properly understand cybersecurity, it must be viewed as the symbiotic relationship between autonomous and manual controls.</td><td>DP04
Design Principle 04:

To properly align industry functions to individual interests, create specialized individual interest inventories that are specific to that industry.</td><td>DP05
Design Principle 05:

Avoid monolithic collectivism of interests for cybersecurity professionals, their interests vary widely in the types of work they prefer to perform.</td><td>DP06
Design Principle 06:

To achieve increased individual satisfaction and performance, properly align individual interests to cybersecurity functions.</td><td>DP07
Design Principle 07:

To develop an artifact within Design Science, the primary focus is to understand and address the challenge.</td></tr>
</table>

5.3 Contribution to Knowledge

The contribution to the body of scientific knowledge goes beyond the original challenge of satisfaction and performance in acquisition and retention. This study required the more specific definition of cybersecurity as a pre-paradigmatic concept, organizational alignment beyond the individual, and individual career development. These concepts and phenomena transcend beyond the original study while maintaining thorough integration throughout. This also includes the contributions to new, or modified, methods of exhibiting design knowledge and theory (Baskerville et al., 2018).

5.3.1 Contribution to Cybersecurity Design Theory

1. Concept of Cybersecurity as an Orchestration Between Manual and Autonomous Systems

The concept that cybersecurity should be seen as an orchestrated effort between manual and autonomous systems became evident. The concept itself, denotes that individuals are not the only entity involved in the selection and execution of security controls. Complex systems that are approaching full autonomy regularly manage security controls. This creates an augmentation of human ability with artificial or predefined logical processes.

2. Cybersecurity and Sociotechnical versus Cyber-Systems

Cybersecurity should be seen as a part of a sociotechnical paradigm of systems. This is because cyber-systems relate to a constrained specificity of control for a purpose that is part of the greater whole of sociotechnical systems. The distinction originally seemed trivial until the implications of a misalignment of these concepts was considered when addressing ambiguity within scientific research. Sociotechnical systems affect an era or society as a whole, while cyber-systems may be seen as one method by which this affect is achieved.

3. Cybersecurity as Battlefield Instead of Business

The analysis of cybersecurity functions reveal that they far more resemble that of battlefield operations than normal business functions. Any discussion of exploitation, attack, defense, deception, and more are reminiscent of the plethora of functions normally found in a cybersecurity career. Within a business environment, deception and attack would be illegal and outside of any regulatory guidance. This generates the need to adjust the paradigm of cybersecurity to both align with business operations, as well as venture beyond normal legal constraints. The actual realization of this process will be determined through practitioner and scientific investigation for some time to come.

5.3.2 Implications of Model for Cybersecurity Careers

1. Cybersecurity Team Restructuring for an Organization

The investigation into cybersecurity functions and organizational structure revealed that functions are often ambiguous, and organizational structure is often poorly defined. This is not to say that any single organizational structure or set of job descriptions will suffice; however, it does indicate the need for additional care and research to be undertaken in planning. An adequate understanding of cybersecurity functions would have a positive impact of the development of cybersecurity structure within an organization and team dynamics.

2. Cybersecurity Career Planning (Secondary, Post-secondary, Change Of Career)

Individuals who attend training courses and advanced education programs would benefit from knowing what types of interests are most closely aligned with various cybersecurity career functions. This would allow students and professionals to potentially avoid years of disappointing work in a position that they would never had pursued had they known the requirements. This knowledge would also allow for the better alignment of cybersecurity training to cybersecurity functions within an organization from educational institutions. In both cases, an individual's ability to choose a more satisfying career is positively impacted.

3. Cybersecurity Increased Satisfaction and Performance

Through the proper alignment of individual interests and cybersecurity functions, both organizations and individuals can experience better performance and satisfaction. This alignment would provide better protection for the organization, as individuals are better equipped to address the threats based on their own innate interests. This would create an environment where more individuals would be hired for properly aligned functions or would be retained for these functions for longer periods of time.

5.4 Assessing the Design of the Cybersecurity Interest-to-Function Career Alignment Model

Special care was taken to methodically conduct this research within prescribed models of design science research, while maintaining a unique individual approach on artifact design. In order to accomplish this, both Hevner's seven Guidelines (Hevner et al., 2004) and Vaishnavi's interpretation of the Design Science Research Process Model (Vaishnavi et al., 2004/2017) were implemented (Table 5-3 The Seven Guidelines of DSRM - Evaluation and

Table 5-4 Knowledge Flow Process and Outputs). Research was also conducted through several conference websites or venue in-person (see Table 5-5 Related Conferences).

Table 5-3 The Seven Guidelines of DSRM - Evaluation

Guideline	Description	Chapters	Application for this Study
Guideline 1	DSR must produce an Artifact	1-2	Artifact 01 Artifact 02 Artifact 03
Guideline 2	Artifact must be relevant to business Problem – Problem special, art developed	3	Cybersecurity Shortage Performance – keeping organizations/companies/people secure Satisfaction – moral obligation Retention
Guideline 3	Design Evaluation	3, 4, 5	Design is tested via Interviews Focus groups Surveys Professional Documentation
Guideline 4	Research Contributions – the problem is solved in a new way	3	Artifacts are developed with clear application to the problems encountered in a new way.
Guideline 5	Research Rigor – Data Collection and Analysis Methods	4, 5	DSR is conducted using rigorous data collection and analysis methods through several technologies.
Guideline 6	Design as a Search Process	3	Several different viewpoints were considered when addressing the problem. The final solution is Guideline 4.
Guideline 7	Communication of Research – Research is presented to a technical and management-oriented audience.	1-5	The results are beneficial to both a technical and business-oriented audience.

Note. Adapted from Design-Science Research Guidelines (Hevner et al., 2004, p. 83)

Table 5-4 Knowledge Flow Process and Outputs

Knowledge Flow	Process	Outputs
	Awareness of Problem	Determination of challenge facing organizations to hire and retain cybersecurity professionals
	Suggestion	Properly align individual interests to cybersecurity functions to improve job satisfaction and organizational performance for cybersecurity professionals.
Several principles are defined	Development	Artifact 01 - Taxonomy of Functions Artifact 02 - Taxonomy of Interests Artifact 03 - Interest-to-Function Alignment
Several propositions are developed	Evaluation	Academic Literature Surveys, Focus Group, Interviews Professional Literature
	Conclusion	It is possible to align individual interests to cybersecurity functions. Literature and individual respondents indicate that this would have a positive impact on employment and retention.

Note. Adapted from Design Science Research Process Model (DSR Cycle) (Vaishnavi et al., 2004/2017, p. 8)

Table 5-5 Related Conferences

Publication/Conference	Description	Website
Society for Industrial and Organizational Psychology (SIOP)	Professional Association I-O Psychology	www.siop.org
Design Science Research in Information Systems and Technology (DESRIST)	Design Science Research Technology	www.desrist.org
International Conference on Cyber Warfare and Security (ICCWS)*	Cybersecurity Cyber Warfare Information Warfare	www.academic-conferences.org/ conferences/iccws/
Institute for Defense and Government Advancement (IDGA)	Cybersecurity For Defense	www.idga.org
GovWare Conference and Exhibition	Cybersecurity Conference Latest Trends	www.govware.sg

* At the 15th Annual International Conference on Cyber Warfare and Security (ICCWS) Conference 2020, the paper entitled, "Psychometric Modelling of Cybersecurity Roles" to the academic audience, and was awarded for the Best PhD Paper (Poteete, 2020) (See Appendix E.2 - ICCWS Best PhD Paper Awarded).

5.5 Limitations and Suggestions for Future Research

This study addressed the challenge of the shortage of cybersecurity professionals from a an important, but constrained viewpoint of an individual's interests within an established set of cybersecurity functions. It is important to realize the limitations that exist with any study involving the infinite possibilities of human nature and organizational purpose, structure, and functions. Additional research in artificial intelligence, machine learning, the Internet of Things, privacy, human rights, and law enforcement could also be beneficial when considering the potential impact on function-to-interest alignment. Also, common factors of job satisfaction when comprised of items such as: salary, location, educational requirements, leadership style, management oversight, culture, and other universal concepts outside of the realm of cybersecurity interests and functions was outside the scope of this research. Concepts involving the general analysis of employee satisfaction, performance, acquisition, and retention may show positive alignment to this research in the future; however, it important to note that an individual cannot be completely isolated to a finite assortment of interests, nor can an organization be reduced to a hierarchy of specific tasks. This was further complicated by the fact that the concept and industry of cybersecurity are pre-paradigmatic. The ambiguity encountered when investigating interests and functions related to cybersecurity within this study was universal. This required that a limited set of artifacts were created to conceptually encapsulate the individual and organizational factors examined throughout this study. This provided a clear solution for the challenges and artifacts defined within this research; however, a multitude of additional viewpoints could also be considered in the future. Also, the artifacts created within this research were not evaluated in actual use within an organization. The real integration of these artifacts within organizations around the world would uncover additional data points that would need further development and analysis. This point is further contemplated by Venable, et al. in the description of ex ante, ex post, naturalistic, and artificial design and evaluation methods (Pries-heje et al., 2008; Venable et al., 2012).

5.6 Conclusion

What began as a model to determine methods to improve individual job satisfaction and organizational retention, expanded to include taxonomies of cybersecurity functions and individual interests. These new challenges, which became prerequisite artifacts to the creation of an integrated artifact that aligned individual interests to cybersecurity functions, required research that exposed the ambiguity within cybersecurity roles and functions across an entire industry. Because of this ambiguity, a discrete set of cybersecurity functions was required in a taxonomy that could be applied to individual interests. The individual interests, as they relate to cybersecurity career functions, were also not defined in academic literature or practitioner publications; therefore, this also required research to create a taxonomy of interests that apply to cybersecurity functions. These two taxonomies became prerequisite artifacts for the integrated final artifact.

In Appendix A-1 Artifact 03 Cybersecurity Interest-to-Function Alignment Model, the taxonomy of interests and functions are shown as part of an integrated artifact. It is also visible that these interests and functions within the integrated artifact provide additional avenues for research and development, in addition to the reality that this research is built upon several decades of exceptional work in a vast array of fields.

As a result, the alignment of an individual's interests to cybersecurity functions is possible and should have a positive impact on personal satisfaction and organizational performance. Literary evidence indicates that these factors should also have a positive effect on retention and acquisition for cybersecurity careers. It is hoped that people from around the world will benefit from a more in-depth understanding of how inherent interests align to organizational functions within cybersecurity; albeit, in the realization that any person can shape their own destiny, and they are not limited by any statistical data.

References

Aken, J. E. van. (2001). Management research on the basis of the design paradigm: The quest for field-tested and grounded technological rules. Journal of Management Studies, 41(2), 219–246.

Alexander, A., & Cummings, J. (2016). The rise of the chief information security officer. People Strategy, 39(1), 10–13.

Allen, D. G. (2006). Do organizational socialization tactics influence newcomer embeddedness and turnover? Journal of Management, 32(2), 237–256.

Alter, S. (2010). Bridging the chasm between sociotechnical and technical views of systems in organizations. Proceedings of JAIS Theory Development Workshop, Sprouts: Working Papers on Information Systems, 9(73), 1–23.

Aruna, M., & Anitha, J. (2015). Employee retention enablers: Generation y employees. SCMS Journal of Indian Management, 12(3), 94–104.

Assante, M. J., & Tobey, D. H. (2011). Enhancing the cybersecurity workforce. IT Professional, 13(1), 12–15.

Bartenschlager, J., & Goeken, M. (2009). Designing artifacts of IT strategy for achieving business/IT-alignment. In 15th Americas Conference on Information Systems 2009, AMCIS 2009 (Vol. 6). San Francisco, CA, USA.

Baskerville, R., Baiyere, A., Gregor, S., Hevner, A. R., & Rossi, M. (2018). Design science research contributions: Finding a balance between artifact and theory. Journal of the Association for Information Systems, 19(5), 358–376.

Baskerville, R., & Pries-Heje, J. (2010). Explanatory design theory. Business & Information Systems Engineering, 2(5), 271–282.

Bassellier, G., & Benbasat, I. (2004). Business competence of information technology professionals: Conceptual development and influence on it-business partnerships. MIS Quarterly, 28(4), 673–694.

Bayazit, N. (2004). Investigating design: A review of forty years of design research. Design Issues, 20(1), 16–29.

Bhattacherjee, A. (2012). Social science research: Principles, methods, and practices (2nd ed.) Textbooks Collection.

Biddle, B. (1986). Recent developments in role theory. Annual Review of Sociology, 12(1), 67–92.

Biggio, G., & Cortese, C. G. (2013). Well-being in the workplace through interaction between individual characteristics and organizational context. International Journal of Qualitative Studies on Health and Well-Being, 8(1), 1–13.

Boddy, A., Hurst, W., Mackay, M., Rhalibi, A. El, Building, J. P., & Street, B. (2017). A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures. Proceedings of the 1st International Conference on Internet of Things and Machine Learning, 1–7. Liverpool, United Kingdom.

Bogner, A., & Menz, W. (2009). The theory-generating expert interview: Epistemological interest, forms of knowledge, interaction. In Interviewing experts (pp. 43–80). Palgrave Macmillan.

Bostrom, R., Gupta, S., & Thomas, D. (2009). A meta-theory for understanding information systems within sociotechnical systems. Journal of Management Information Systems, 26(1), 17–48.

Bowen, P., Hash, J., Wilson, M., Gutierrez, C. M., & Jeffrey, W. (2006). Information security handbook: A guide for managers. In NIST Special Publication (SP) 800-100.

Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. Computers & Security, 88(101607), 1–13.

Caldwell, T. (2013). Plugging the cybersecurity skills gap. Computer Fraud & Security, 7, 5–10.

Campbell, B. (2005). Alignment: Resolving ambiguity within bounded choices. In 9th Pacific Asia Conference on Information Systems: I.T. and Value Creation, PACIS 2005.

Campbell, B. (2008). The intractable nature of alignment. ACIS 2008 Proceedings - 19th Australasian Conference on Information Systems, 166–175, Christchurch, New Zealand.

Campbell, S. G., O’Rourke, P., & Bunting, M. F. (2015). Identifying dimensions of cyber aptitude: The design of the cyber aptitude and talent assessment. Proceedings of the Human Factors and Ergonomics Society, 59(1), 721–725.

Chamberlain, T. C., Catano, V. M., & Cunningham, D. P. (2005). Personality as a predictor of professional behavior in dental school: Comparisons with dental practitioners. Journal of Dental Education, 69(11), 1222–1237.

Chan, Y. E. (2002). Why haven’t we mastered alignment? The importance of the information organization structure. MIS Quarterly, 1(2), 97–112.

Chen, J., & Neo, P. (2019). Texting the waters: An assessment of focus groups conducted via the WhatsApp smartphone messaging application. Methodological Innovations, 12(3), 1-10.

Clarke, V., & Braun, V. (2017). Thematic analysis. The Journal of Positive Psychology, 12(3), 1–2.

Colquitt, J. A., Scott, B. A., & LePine, J. A. (2007). Trust, trustworthiness, and trust propensity: a meta-analytic test of their unique relationships with risk taking and job performance. The Journal of Applied Psychology, 92(4), 909–927.

Colwill, C. (2009). Human factors in information security: The insider threat - Who can you trust these days? Information Security Technical Report, 14(4), 186–196.

Colwill, C., & Jones, A. (2007). The importance of human factors when assessing outsourcing security risks. In Proceedings of the 5th Australian Information Security Management Conference (pp. 47–52). Perth Western, Australia.

Cooke, N. M., & McDonald, J. E. (1986). A formal methodology for acquiring and representing expert knowledge. Proceedings of the IEEE, 74(10), 1422–1430.

Cowan, D. (2003). Informatics for the clinical laboratory: A practical guide. Springer.

Creswell, J. W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches (3rd ed.) SAGE Publishing.

Crumpler, W., & Lewis, J. A. (2019). The cybersecurity workforce gap. Center for Strategic and International Studies, July 2016, 1–10. Retrieved from http://www.isaca.org/Knowledge-Center/

Curran, P. (2016). Cyber security today: Career paths, salaries and in-demand job titles. Checkmarx. Retrieved from https://www.checkmarx.com/2016/08/30/cyber-security-career-paths-salaries-and-the-most-in-demand-job-titles/

Cyber security degrees and careers. (n.d.). Learn How to Become. Retrieved July 1, 2020, from https://www.learnhowtobecome.org/computer-careers/cyber-security/

Cybersec jobs. (n.d.). Cyber Sec Jobs. Retrieved July 1, 2020, from https://cybersecjobs.com/

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. Frontiers in Psychology, 9(JUN), 1–12.

De Haes, S., & Van Grembergen, W. (2004). IT governance and its mechanisms. Information Systems Audit and Control Association, 1.

Deci, E. L., & Ryan, R. M. (2008). Self-determination theory: A macrotheory of human motivation, development, and health. Canadian Psychology, 49(3), 182–185.

Deng, Q., Wang, Y., & Ji, S. (2017). Design science research in information systems: A systematic literature review 2001 to 2015. International Conference on Information Resources Management (CONF-IRM), 13. Santiago, Chile.

Department of Computer Science. (n.d.). Cybersecurity roles and job titles. George Washington University. Retrieved June 4, 2018, from https://www.cs.seas.gwu.edu/cybersecurity-roles-and-job-titles

Department of the United States Army. (2014). Cyber electromagnetic activities (FM 3-38). Cyber electromagnetic activities (FM 3-38).

Design Science Research in Information Systems and Technology (DESRIST). (2015) Conferences. Retrieved from June 3, 2019 from http://desrist.org/conference/

DeSilver, D. (2014). How U.S. tech-sector jobs have grown, changed in 15 years. S. tech-sector jobs have grown, changed in 15 years. Pew Research Center. Retrieved from http://pewrsr.ch/PtqZDA

Digman, J. M. (1990). Personality structure: Emergence of the five-factor model. Annual Review of Psychology, 41(1), 417–440.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security, 4, 92–100.

Dodge, R., Toregas, C., & Hoffman, L. J. (2012). Cybersecurity workforce development directions. In Proceedings of the 6th International Symposium on Human Aspects of Information Security and Assurance, HAISA (pp. 1–12), Berlin Heidelberg: Springer.

Doyle, A. (2019). IT jobs: Career options, job titles, and descriptions. The Balance Careers. Retrieved from https://www.thebalancecareers.com/list-of-information-technology-it-job-titles-2061498

Dreibelbis, R. C., Martin, J., Coovert, M. D., & Dorsey, D. W. (2018). The looming cybersecurity crisis and what It means for the practice of industrial and organizational psychology. Industrial and Organizational Psychology, 11(2), 346–365.

Edwards, J. R., Caplan, R. D., & Harrison, R. Van. (1998). Person-environment fit theory: Conceptual foundations, empirical evidence, and directions for future research. In C. L. Cooper (Ed.), Theories of organizational stress (Vol. 53, Issue 9, pp. 28–67). Oxford: Oxford University Press.

Emery, F. (1982). Socio-technical foundations for a new social order? Human Relations, 35(12), 1095–1122.

Evans, J. R., & Mathur, A. (2005). The value of online surveys. Internet Research, 15(2), 195–219.

Executive Office of the President of the U.S. (2009). Cyberspace policy review, Assuring a trusted and resilient information and communications infrastructure. 76.

Fine, S. A., & Getkate, M. (1995). Benchmark tasks for job analysis: A guide for Functional Job Analysis (FJA) scales. Psychology Press.

Francis, K. A., & Ginsberg, W. (2016). The federal cybersecurity workforce: Background and congressional oversight issues for the Departments of Defense and Homeland Security (CRS Report R44338). Congressional Research Service.

Fuller, R. B. (1957). A comprehensive anticipatory design science. Royal Architectural Institute of Canada, 34(9), 357.

Fuller, R. B. (1963). Phase I document 1: Inventory of world resources, human trends, and needs. In J. McHale (Ed.), World design science decade (pp. 1965–1975). World Resources Inventory, Southern Illinois University.

Fuller, R. B. (1983). Humanity's critical path: From weaponry to livingry.

Galton, F. (1884). Measurement of character. Fortnightly Review, 36, 179–185.

Gati, I., Krausz, M., & Osipow, S. H. (1996). A taxonomy of difficulties in career decision making. Journal of Counseling Psychology, 43(4), 510–526.

Ghapanchi, A. H., & Aurum, A. (2011). Antecedents to IT personnel's intentions to leave: A systematic literature review. Journal of Systems and Software, 84(2), 238–249.

Ghapanchi, A. H., Ghapanchi, A. R., Talaei-Khoei, A., & Abedin, B. (2013). A systematic review on information technology personnel's turnover. Lecture Notes on Software Engineering, 1(1), 98–101.

Goldberg, L. R. (1990). An alternative description of personality: The Big-Five factor structure. Journal of Personality and Social Psychology, 59(6), 1216–1229.

Goldberg, L. R. (1998). In memoriam Warren T. Norman (1930–1998): An appreciation. Journal of Research in Personality, 32, 391–396.

Goldberg, L. R. (1999). A broad-bandwidth, public-domain, personality inventory measuring the lower level facets of several Five-Factor models. In Personality Psychology in Europe (Vol. 7, pp. 7–28).

Greene, S. S. (2014). Security program and policies: Principles and practices (D. Dusthimer (Ed.); 2nd ed.). Pearson.

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. MIS Quarterly, 37(2), 337–355.

Gregor, S., & Jones, D. (2007). The anatomy of a design theory. Journal of the Association for Information Systems, 8(5), 313–335.

Gregor, S., Kruse, L. C., & Seidel, S. (2020). The anatomy of a design principle. Journal of the Association for Information Systems, 21(6), 1622-1652.

Gregory, S. A. (1966). The design method. Springer.

Guest, G., Macqueen, K. M., & Namey, E. E. (2012). Introduction to applied thematic analysis. In Applied Thematic Analysis (pp. 3–20). SAGE Publications, Inc.

Guzman, I.R. & Stanton, J. M. (2009). IT occupational culture: The cultural fit and commitment of new information technologists. Information Technology & People 22(2), 157-187.

Hackman, J. R., & Oldham, G. R. (1975). Development of the Job Diagnostic Survey. Journal of Applied Psychology, 60, 159–170.

Hackman, J. R., & Oldham, G. R. (1976). Motivation through the design of work: Test of a theory. Organizational Behavior and Human Performance, 16(2), 250–279.

Hamilton, R. J., & Bowers, B. J. (2006). Internet recruitment and e-mail interviews in qualitative studies. Qualitative Health Research, 16(6), 821–835.

Hardigan, P. C., Cohen, S. R., & Carvajal, M. J. (2001). Linking job satisfaction and career choice with personality styles: An exploratory study of practicing pharmacists. Journal of Psychological Type, 57, 30–35.

Heavey, A. L., Holwerda, J. A., & Hausknecht, J. P. (2013). Causes and consequences of collective turnover: A meta-analytic review. Journal of Applied Psychology, 98(3), 412–453.

Hernandez, L. F., & Johnson, D. K. (2014). Designing incentives for Marine Corps cyber workforce retention. In Naval Postgraduate School.

Hevner, A. R. (2007). A three cycle view of design science research. Scandinavian Journal of Information Systems, 19(2), 87–92.

Hevner, A. R., & Chatterjee, S. (2010). Design science research in information systems. In Design Research in Information Systems. Integrated Series in Information Systems (Vol. 22, pp. 75–105). Springer.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105.

Holland, J. L. (1986). 9. New directions for interest testing. In B. Witt, S. Plake, & J. C. (Eds.), The future of testing (Vol. 2, pp. 245–267).

Holmström, J., Ketokivi, M., & Hameri, A. P. (2009). Bridging practice and theory: A design science approach. Decision Sciences, 40(1), 65–87.

Holtom, B. C., Mitchell, T. R., Lee, T. W., & Eberly, M. B. (2008). Turnover and retention research: A glance at the past, a closer review of the present, and a venture into the future. The Academy of Management Annals, 2(1), 231–274.

Hom, P. W., Lee, T. W., Shaw, J. D., & Hausknecht, J. P. (2017). One hundred years of employee turnover theory and research. Journal of Applied Psychology, 102(3), 530–545.

Hoyt, J. (2011). Sectitles (p.Sectitles (p. Python Script). Retrieved November 25, 2018 from https://cdn.zeltser.com/media/archive/infosec-job-titles-script.txt

Hulin, C. (1991). Adaptation, persistence, and commitment in organizations. In M. D. Dunnette & L. M. Hough (Eds.), Handbook of industrial and organizational psychology (2nd ed., Vol. 1, pp. 445–506). Consulting Psychologists Press, Inc.

Iivari, J. (2005). Information systems as a design science. In O. Vasilecas, W. Wojtkowski, J. Zupančič, A. Caplinskas, W. G. Wojtkowski, & S. Wrycza (Eds.), Information systems development (pp. 15–27). Springer.

Information Systems Audit and Control Association (ISACA). (2018). State of cybersecurity 2018. State of Cybersecurity 2018: Workforce Development.

Infosec Institute. (2018). Job titles. Retrieved July 15 2019 from https://resources.infosecinstitute.com/job-titles/

InfoSec Institute. (2020). Build your cybersecurity workforce.

International Information System Security Certification Consortium (ISC)2. (2018). Hiring and retaining top cybersecurity talent.

International Information System Security Certification Consortium (ISC)2. (2019). Strategies for building and growing strong cybersecurity teams. In (ISC)2 Cybersecurity workforce study.

Irizarry, R. (2020). Introduction to data science: Data analysis and prediction algorithms with R. CRC Press.

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission). (2014). Information technology — Security techniques — Information security management systems — Overview and vocabulary. In International organization for standardization (3rd ed.). ISO/IEC 27000.

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission). (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. In ACM Workshop on formal methods in security engineering (5th ed., Vol. 34, Issue 19). ISO/IEC 27000.

Jackson, D. N., Holden, R. R., Locklin, R. H., & Marks, E. (1984). Taxonomy of vocational interests of academic major areas. Journal of Educational Measurement, 21(3), 261–275.

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360.

Jigău, M. (2007). Career counselling: Compendium of methods and techniques. AFIR.

John, O. P., Robins, R. W., & Pervin, L. A. (2008). Handbook of personality theory and research. In Handbook of personality (3rd ed.). The Guilford Press.

Johnson, T. W., & Stinson, J. E. (1975). Role ambiguity, role conflict, and satisfaction: Moderating effects of individual differences. The Journal of Applied Psychology, 60(3), 329–333.

Joint Task Force Transformation Initiative. (2014). Assessing security and privacy controls in federal information systems and organizations building effective assessment plans. In NIST Special Publication (SP) 800-53A.

Joseph, D., Boh, W. F., Ang, S., & Slaughter, S. A. (2012). The career paths less (or more) traveled: A sequence analysis of IT career histories, mobility patterns, and career success. MIS Quarterly, 36(2), 427–452.

Joseph, D., Ng, K.-Y., Koh, C., & Ang, S. (2007). Turnover of information technology professionals: A narrative review, meta-analytic structural equation modeling, and model development. MIS Quarterly, 31(3), 547–577.

Judge, T. A., Higgins, C. A., Thoresen, C. J., & Barrick, M. R. (1999). The Big Five personality traits, general mental ability, and career success across the life span. Personnel Psychology, 52(3), 621–652.

Jung, C. G. (1921). Psychological types. In Collected works of C.G. Jung (Vol. 6, p. 198). Princeton University Press.

Kaelin, M. (2018). 10 Signs you may not be cut out for a cybersecurity job. TechRepublic. Retrieved July 1, 2020 from https://www.techrepublic.com/article/10-signs-you-arent-cut-out-to-be-a-cybersecurity-specialist/?ftag=TRE684d531&bhid=28057947887427018440504385342394

Katz, D., & Kahn, R. L. (1978). The social psychology of organizations. Wiley.

Kauffman, R. J., & Josefek, R. A. (2003). IT human capital and the information systems professional's decision to leave the company. Mobile Media and Communication. 8(2), 229-246

Kaufman, J. C., Pumaccahua, T. T., & Holt, R. E. (2013). Personality and creativity in realistic, investigative, artistic, social, and enterprising college majors. Personality and Individual Differences, 54(8), 913–917.

Kelland, M. (2017). Personality theory. OER Commons. Retrieved from https://www.oercommons.org/authoring/22859-personality-theory/4/view#

Kennedy, B., Curtis, K., & Waters, D. (2014). Is there a relationship between personality and choice of nursing specialty: An integrative literature review. BMC Nursing, 13(40).

Klement, M., Chráska, M., & Chrásková, M. (2015). The use of the semantic differential method in identifying the opinions of university students on education realized through e-learning. Procedia - Social and Behavioral Sciences, 186, 1214–1223.

Kuechler, B., & Vaishnavi, V. (2008). Theory development in design science research: Anatomy of a research project. European Journal of Information Systems, 17(5), 489–504.

Kuechler, V., Kuechler, W., & Petter, S. (2004). Design science research in information systems. 1, 1–66.

Kuechler, W., & Vaishnavi, V. (2012). A framework for theory development in design science research: Multiple perspectives. Journal of the Association for Information Systems, 13(6), 395–423.

Lee, T. W., & Mitchell, T. R. (1994). Organizational attachment: Attitudes and actions. In J. Greenberg (Ed.), Series in applied psychology. Organizational behavior: The state of the science (pp. 83–108).Lawrence Erlbaum Associates, Inc.

Lefever, S., Dal, M., & Matthíasdóttir, Á. (2007). Online data collection in academic research: Advantages and limitations. British Journal of Educational Technology, 38(4), 574–582.

Leggitt, J. S., Shechter, O. G., & Lang, E. L. (2011). Cyberculture and personnel security: Report 1-orientation, concerns, and needs. Defense Personnel Security Research Center, Department of Defense, U.S.

Lewis, P., & Rivkin, D. (1999). Development of the O*NET interest profiler. In National Center for O*NET Development.

Lewis, P., & Rivkin, D. (2000). O*NET interest profiler user's guide (3rd ed. U.S. Department of Labor, Employment and Training Administration.

Liao, H. Y., Armstrong, P. I., & Rounds, J. (2008). Development and initial validation of public domain Basic Interest Markers. Journal of Vocational Behavior, 73(1), 159–183.

Libicki, M. C., Senty, D., & Pollak, J. (2014). H4CKER5 wanted: An examination of the cybersecurity labor market. RAND Corporation.

Lin, Y., Michel, J.-B., Lieberman Aiden, E., Orwant, J., Brockman, W., & Petrov, S. (2012). Syntactic annotations for the Google Books Ngram Corpus. In Proceedings of the 50th Annual Meeting of the Association for Computational Linguistics (Issue 2).

Locke, G., & Gallagher, P. D. (2011). Managing information security risk: Organization, mission, and information system view. NIST Special Publication (SP) 800-39, 88.

Lunenburg, F. C. (2011). Motivating by enriching jobs to make them more interesting and challenging. International Journal of Management, Business, and Administration, 15(1), 1–11.

Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. Information and Computer Security, 27(2), 233–272.

March, J. G., & Simon, H. A. (1958). Organizations. Wiley.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. Decision Support Systems, 15(4), 251–266.

March, S. T., & Storey, V. C. (2008). Design science in the information systems discipline: An introduction to the special issue on design science research. MIS Quarterly, 32(4), 725–730.

Martini, B., & Choo, K. K. R. (2014). Building the next generation of cyber security professionals. In Twenty Second European Conference on Information Systems, Tel Aviv, Israel.

Mayring, P. (2020). Qualitative content analysis: Demarcation, varieties, developments. Qualitative Social Research, 20(3). 1-15.

McAdams, D. P. (1992). The Five-Factor Model in personality: A critical appraisal. Journal of Personality, 60(2), 329–361.

McAfee. (2016). Hacking the skills shortage: A study of the international shortage in cybersecurity skills. Center for Strategic and International Studies, 1-14.

McClain, J., Silva, A., Emmanuel, G., Anderson, B., Nauer, K., Abbott, R., & Forsythe, C. (2015). Human performance factors in cyber security forensic analysis. Procedia Manufacturing, 3, 5301–5307.

McDaniel, M. A., & Snell, A. F. (1999). Holland’s theory and occupational information. Journal of Vocational Behavior, 55(1), 74–85.

Meeusen, V., Van Dam, K., Brown-Mahoney, C., Van Zundert, A., & Knape, H. (2010). Burnout, psychosomatic symptoms and job satisfaction among Dutch nurse anaesthetists: A survey. In Risk factors for job turnover among Dutch nurse anaesthetists: The influence of job satisfaction, work climate, work context and personality dimensions (pp. 616–621). Acta Anaesthesiol.

Mikolic-Torreira, I., Henry, R., Snyder, D., Beaghley, S., Pettyjohn, S., Harting, S., Westerman, E., Shlapak, D., Bishop, M., Oberholtzer, J., Skrabala, L., & Weinbaum, C. (2016). A framework for exploring cybersecurity policy options. RAND Corporation.

Mingers, J. (2001). Combining IS research methods: Towards a pluralist methodology. Information Systems Research, 12(3), 240–259.

Mitchell, T. R., & Lee, T. W. (2001). The unfolding model of voluntary turnover and job embeddedness: Foundations for a comprehensive theory of attachment. Research in Organizational Behavior, 23, 189–246.

Mitnick, B. M. (1976). The theory of agency: A framework. Annual Meeting of the American Sociological Association.

Mobley, W. H. (1977). Intermediate linkages in the relationship between job satisfaction and employee turnover. Journal of Applied Psychology, 62(2), 237–240.

Morgan, D. L. (1996). Focus groups. Annual Review of Sociology, 22(1), 129–152.

Morgan, S. (2016). Top 10 IT security jobs and salaries. Forbes. Retrieved from https://www.forbes.com/sites/stevemorgan/2016/04/12/top-10-it-security-jobs-and-salaries/#6e8cf2467136

Morgeson, F. P., & Campion, M. A. (2000). Accuracy in job analysis: Toward an inference-based model. Journal of Organizational Behavior, 21(7), 819–827.

Morgeson, F. P., Campion, M. A., Dipboye, R. L., Hollenbeck, J. R., Murphy, K., & Schmitt, N. (2007). Are we getting fooled again? Coming to terms with limitations in the use of personality tests for personnel selection. Personnel Psychology, 60, 1029–1049.

Mowday, R. T., Steers, R. M., & Porter, L. W. (1979). Employee turnover and post-decision accommodation process. In University of Oregon.

Myers, I. B. (2016). Introduction to type: A guide to understanding your results on the MBTI instrument (7th ed.). Consulting Psychologists Press. (Original work published 1962)

Myers, M. D. (2013). Qualitative research in business & management (2nd ed.). SAGE Publishing.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. Information and Organization, 17(1), 2–26.

Naidoo, R. (2016). A communicative-tension model of change-induced collective voluntary turnover in IT. The Journal of Strategic Information Systems, 25(4), 277–298.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. European Journal of Information Systems, 29(3), 306-321.

National Institute of Standards and Technology (NIST). (2020). Security and privacy controls for federal information systems and organizations. In NIST Special Publication (SP) 800-53 Rev. 5. US Department of Commerce.

Nauta, M. M. (2010). The development, evolution, and status of Holland’s theory of vocational personalities: Reflections and future directions for counseling psychology. Journal of Counseling Psychology, 57(1), 11–22.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework. In NIST Special Publication (SP) 800-181.

Nickerson, R. C., Muntermann, J., & Varshney, U. (2010). Taxonomy development in information systems: A literature survey and problem statement. In 16th Americas Conference on Information Systems 2010, AMCIS 2010 (Vol. 5), Lima, Peru.

Nickerson, R. C., Varshney, U., Muntermann, J., & Issac, H. (2009). Taxonomy development in information systems: Developing a taxonomy of mobile applications. Information Systems, January, 1–13.

Norman, W. T. (1967). 2800 personality trait descriptors: Normative operating characteristics for a university population. University of Michigan.

Nunamaker, J., Chen, M., & Purdin, T. (1990). Systems development in information systems research. Journal of Management Information Systems, 7(3), 89–106.

Offermann, P., Levina, O., Schönherr, M., & Bub, U. (2009). Outline of a design science research process. Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology, 1–11, Malvern, PA, USA.

Ogbanufe, O., & Spears, J. (2019). Burnout in cybersecurity professionals. Proceedings of the 14th Pre-ICIS Workshop on Information Security and Privacy, 1–10, Munich, Germany.

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. Sprouts: Working Papers on Information Systems, 10(26), 10–26.

Olson, J. M., & Maio, G. R. (2003). Attitudes in social behavior. In I. B. Weiner, T. Millon, & M. J. Lerner (Eds.), Handbook of psychology, volume V: personality and social psychology (Vol. 5, pp. 299–325). John Wiley & Sons, Inc.

Oltsik, J. (2019). The life and times of cybersecurity professionals. Enterprise Strategy Group.

Onita, C., & Dhaliwal, J. (2011). Alignment within the corporate IT unit: An analysis of software testing and development. European Journal of Information Systems, 20(1), 48–68.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. Information Systems Research, 2(1), 1–28.

Otero, A. R. (2018). Information technology control and audit (5th ed.). CRC Press.

Oudeyer, P. Y., & Kaplan, F. (2007). What is intrinsic motivation? A typology of computational approaches. Frontiers in Neurorobotics, 1(6), 1-2.

Paller, A. (2020). SANS NewsBites. SANS Institute, 22(74), 1–18.

Park, T.-Y., & Shaw, J. D. (2013). Turnover rates and organizational performance: Review, critique, and research agenda. The Journal of Applied Psychology, 98(2), 268–309.

Parker, A., & Brown, I. (2019). Skills requirements for cyber security professionals: A content analysis of job descriptions in South Africa. Communications in Computer and Information Science, 973, 176–192.

Peffers, K., Tuunanen, T., & Niehaves, B. (2018). Design science research genres: Introduction to the special issue on exemplars and criteria for applicable design science research. European Journal of Information Systems, 27(2), 129–139.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems, 24(3), 44–77.

Petrides, K. V., & McManus, I. C. (2004). Mapping medical careers: Questionnaire assessment of career preferences in medical school applicants and final-year students. BMC Medical Education.

Ping-Ju Wu, S., Straub, D. W., & Liang, T.-P. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. MIS Quarterly, 39(2), 497–518.

Porter, L. W., & Steers, R. M. (1973). Organizational, work, and personal factors in employee turnover and absenteeism. Psychological Bulletin, 80(2), 151–176.

Poteete, P. W. (2020). Psychometric modelling of cybersecurity roles. In B. K. Payne & H. Wu (Eds.), Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020 (pp. 530–538). Academic Conferences and Publishing International: Norfolk, VA, USA.

Pries-heje, J., Baskerville, R., & Venable, J. R. (2008). Strategies for Design Science Research Evaluation. In Proceedings of the European Conference on Information Systems - ECIS 2008: Galway, Ireland.

Ramirez, R., & Choucri, N. (2016). Improving interdisciplinary communication with standardized cyber security terminology: A literature review. IEEE Access, 4, 2216–2243.

Rayman, J. R. (The P. S. U. (2008). A tribute to John L. Holland: Psychologist, theoretician, scholar, researcher, counselor, and friend. National Career Development Association (NCDA).

Retrieved July 1, 2020 from https://associationdatabase.com/aws/NCDA/pt/sd/news_article/6521/_PARENT/layout_details/false

Revelle, W. (2014). Francis Galton. In The encyclopedia of clinical psychology. Wiley-Blackwell.

Rizzo, J. R., House, R. J., & Lirtzman, S. I. (1970). Role conflict and ambiguity in complex organizations. Administrative Science Quarterly, 15(2), 150–163.

Rothstein, M. G., & Goffin, R. D. (2006). The use of personality measures in personnel selection: What does current research support? Human Resource Management Review, 16(2), 155–180.

Rounds, J., & Walker, C. (1999). O*NET Interest Profiler: Reliability, validity, and self-scoring. Center for O*NET. Retrieved from http://prod-02.onetcenter.org/center/dl_files/IP_RVS.pdf

Ryan, R. M., & Deci, E. L. (2000). Intrinsic and extrinsic motivations: Classic definitions and new directions. Contemporary Educational Psychology, 25, 54–67.

Said, A. R., Abdullah, H., Uli, J., & Mohamed, Z. A. (2014). Relationship between organizational characteristics and information security knowledge management implementation. Procedia Social and Behavioral Sciences, 123, 433–443.

Saldaña, J. (2015). The coding manual for qualitative researchers (2nd ed.). SAGE Publishing.

SANS Institute. (1989). SysAdmin Audit, Network, and Security (SANS) Institute. Retrieved from https://www.sans.org/about/

Schlosser, F., Beimborn, D., Weitzel, T., & Wagner, H. T. (2015). Achieving social alignment between business and IT - An empirical evaluation of the efficacy of IT governance mechanisms. Journal of Information Technology, 30(2), 119–135.

Security Wizardry. (2018). Security roles defined. Computer Network Defense. Retrieved from https://www.securitywizardry.com/10-recruitment/recruitment/60-security-roles-defined

Sein, M., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. MIS Quarterly, 35(1), 37–56.

Selm, M. V. A. N., & Jankowski, N. W. (2006). Conducting online surveys. Quality and Quantity, 40(3), 435–456.

Shahzad, B., Abdullatif, A. M., Saleem, K., & Jameel, W. (2017). Socio-technical challenges and mitigation guidelines in developing mobile healthcare applications. Journal of Medical Imaging and Health Informatics, 7(2), 1–9.

Shapiro, S. P. (2005). Agency Theory. Annual Review of Sociology, 31, 263–284.

Simon, H. A. (1996). The sciences of the artificial (3rd ed.). MIT Press.

Singh, N., & Sharma, L. S. (2015). Process models of employee turnover during 1975-1995: A review. European Academic Research, 3(2), 2494–2518. www.euacademic.org.

Sommestad, T., Ekstedt, M., & Johnson, P. (2009). Cyber security risks assessment with bayesian defense graphs and architectural models. In Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS. IEEE, Waikoloa, Big Island, HI, USA.

Sørensen, H. T., Sabroe, S., & Olsen, J. (1996). A framework for evaluation of secondary data sources for epidemiological research. International Journal of Epidemiology, 25(2), 435–442.

Steers, R. M., & Mowday, R. T. (1981). Employee turnover and post-decision accommodation processes. In L.L. Cummings & B.M. Staw (Eds.), Research in organizational behavior (Vol. 3, pp. 235–282). JAI Press.

Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. Politics and Governance, 6(2), 1–4.

Stewart, K., & Williams, M. (2005). Researching online populations: The use of online focus groups for social research. Qualitative Research, 5(4), 395–416.

Stine, K., Kissel, R., Barker, W. C., Fahlsing, J., & Gulick, J. (2002). Volume I: Guide for mapping types of information and information systems to security categories. NIST Special Publication (SP) 800-60, 1, 53.

Stine, K., Kissel, R., Barker, W. C., Lee, A., & Fahlsing, J. (2008). Volume II: Appendices to guide for mapping types of information and information systems to security categories. NIST Special Publication (SP) 800-60, 2, 304.

Taylor, R. G., & Campbell, D. P. (1969). A comparison of the SVIB basic interest scales with the regular occupational scales. The Personnel and Guidance Journal, 47(5), 450–455.

Tett, R. P., & Jackson, D. N. (1991). Personality measures as predictors of job performance: A meta-analytic review in an important review of the validity of personality measures in personnel selection. Personnel Psychology, 44(4), 703–742.

The White House. (2018). National cyber strategy of the United States of America. Office of the President of the United States, 40.

Thuan, N. H., Drechsler, A., & Antunes, P. (2019). Construction of design science research questions. Communications of the Association for Information Systems, 44(1), 332–363.

Tiene, D. (2000). Online discussions: A survey of advantages and disadvantages compared to face-to-face discussions. Journal of Educational Multimedia and Hypermedia, 9(4), 369–382.

Tokar, D. M., Vaux, A., & Swanson, J. L. (1995). Dimensions relating Hollands vocational personality typology and the 5-factor model. Journal of Career Assessment, 3(1), 57–74.

Top 10 security careers. (n.d.). Security Degree Hub. Retrieved July 1, 2020, from https://www.securitydegreehub.com/top-security-careers/

Trist, E. (1981). The evolution of socio-technical systems: A conceptual framework and action research program. In A. H. V. De V. William F. Joyce (Ed.), Perspectives on organization design and behavior (pp. 19–75). Wiley.

Ulum, M. (2018). Literature review on cyber security discourse. February 2017.

Vaishnavi, V., & Kuechler, W. (2008). Introduction to design science research in information and communication technology. In Design science research methods and patterns-innovating information and communication technology (pp. 7–30). Taylor & Francis Group.

Vaishnavi, V., & Kuechler, W. (2015). Design science research methods and patterns: Innovating information and communication technology (2nd ed.). CRC Press.

Vaishnavi, V., Kuechler, W., & Petter, S. (2017). Design science research in information systems. Retrieved July 20, 2020 Retrieved from http://www.desrist.org/design-research-in-information-systems/ (Original work published 2004).

Venable, J. R., Pries-Heje, J., & Baskerville, R. (2012). A comprehensive framework for evaluation in design science research. In K. Peffers, B. Kuechler, & M. Rothenberger (Eds.), International Conference on Design Science in Information Systems (pp. 423–438). Springer.

Venable, J. R., Pries-Heje, J., & Baskerville, R. (2016). FEDS: A framework for evaluation in design science research. European Journal of Information Systems, 25(1), 77–89.

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? Computers and Security, 24(2), 99–104.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers and Security, 38, 97–102.

Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an information system design theory for vigilant EIS. Information Systems Research, 3(1), 36–59.

Webster, J., & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. MIS Quarterly, 26(2), 13–23.

WeiBo, Z., Kaur, S., & Zhi, T. (2010). A critical review of employee turnover model (1938- 2009) and development in perspective of performance. African Journal of Business Management, 4(19), 4146–4158.

Weill, P., & Ross, J. W. (2005). A matrixed approach to designing IT governance. MIT Sloan Management Review, 46(2), 26–34.

Wiener, N. (2019). Cybernetics: Or control and communication in the animal and the machine (2nd ed.). MIT Press.

Wilk, S. L., & Sackett, P. R. (1996). Longitudinal analysis of ability-job complexity fit and job change. Personnel Psychology, 49(4), 937–967.

Wille, B., De Fruyt, F., & Feys, M. (2010). Vocational interests and Big Five traits as predictors of job instability. Journal of Vocational Behavior. 76(3), 547-558.

Winter, R. (2008). Design science research in Europe. European Journal of Information Systems, 17(5), 470–475.

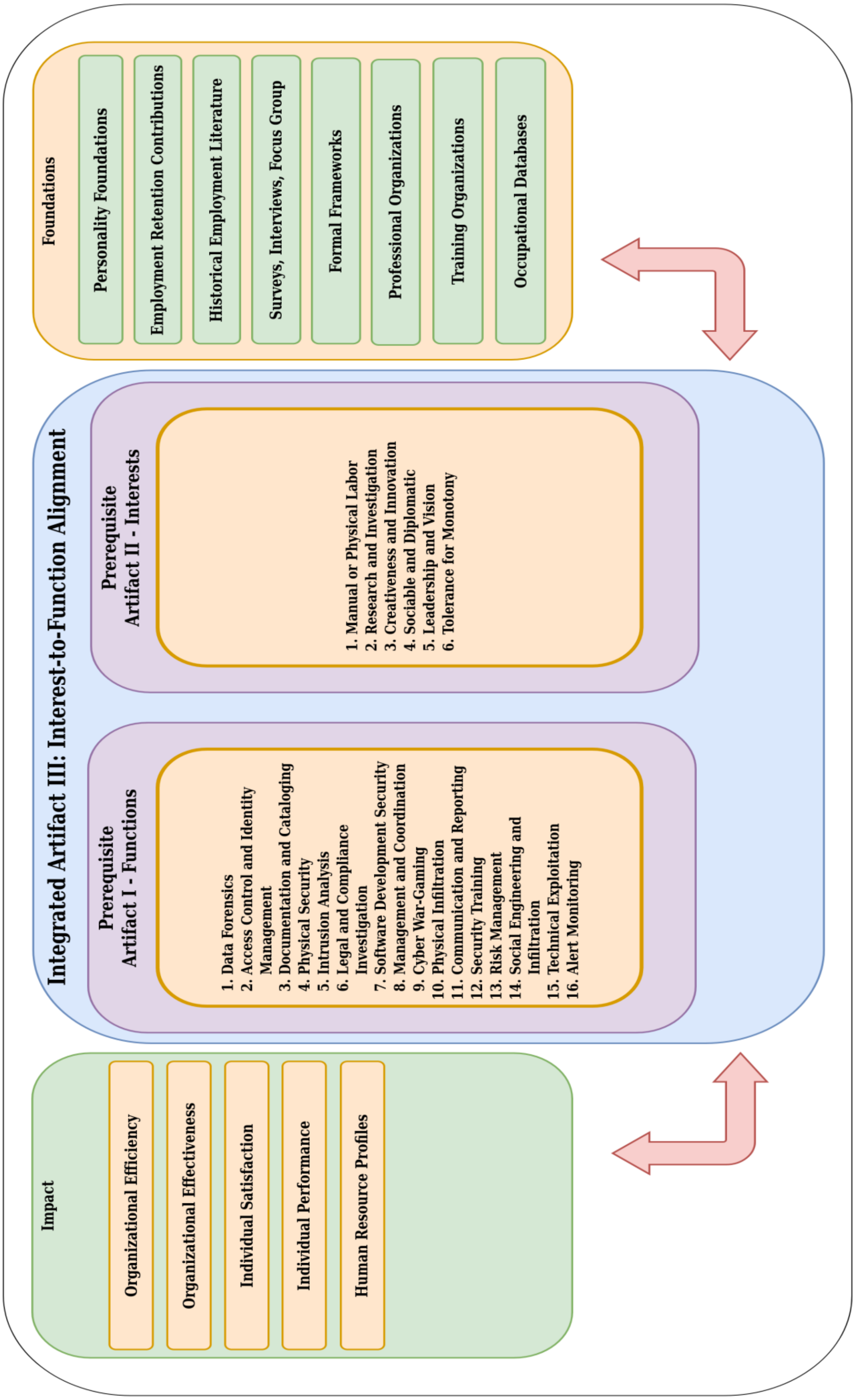
Workforce Intelligence Network (WIN). (2017). Cybersecurity skills gap analysis, National and advance Michigan region data.

Wu, P. P. Y., Fookes, C., Pitchforth, J., & Mengersen, K. (2015). A framework for model integration and holistic modelling of socio-technical systems. Decision Support Systems, 71, 14–27.

Zeltser, L., & Hoyt, J. (2015). Which information security job titles are least and most common? Retrieved November 24, 2019 from https://zeltser.com/information-security-job-titles-popularity/

Appendix

A.1 Artifact 03 Cybersecurity Interest-to-Function Alignment Model


Foundations
Personality Foundations
Employment Retention Contributions
Historical Employment Literature
Surveys, Interviews, Focus Group
Formal Frameworks
Professional Organizations
Training Organizations
Occupational Databases
Integrated Artifact III: Interest-to-Function Alignment
Prerequisite
Artifact II - Interests
1. Manual or Physical Labor
2. Research and Investigation
3. Creativeness and Innovation
4. Sociable and Diplomatic
5. Leadership and Vision
6. Tolerance for Monotony
Prerequisite
Artifact I - Functions
1. Data Forensics
2. Access Control and Identity Management
3. Documentation and Cataloging
4. Physical Security
5. Intrusion Analysis
6. Legal and Compliance Investigation
7. Software Development Security
8. Management and Coordination
9. Cyber War-Gaming
10. Physical Infiltration
11. Communication and Reporting
12. Security Training
13. Risk Management
14. Social Engineering and Infiltration
15. Technical Exploitation
16. Alert Monitoring
Impact
Organizational Efficiency
Organizational Effectiveness
Individual Satisfaction
Individual Performance
Human Resource Profiles

A.2 Job Titles - Thirteen Sources

	http://blog.zeltser.com/post/4832658181/information-security-job-titles-	https://doi.org/10.6028/NIST.SP.800-181	https://www.cs.seas.gwu.edu/cybersecurity-roles-and-job-titles	https://www.checkmarx.com/2016/08/30/cyber-security-career-paths-	http://www.cyberdegrees.org/jobs/	https://www.forbes.com/sites/stevemorgan/2016/04/12/top-10-it-security-	https://www.thebalance.com/list-of-information-technology-it-job-titles	https://www.learnhowtobecome.org/computer-careers/cyber-security/	https://www.techrepublic.com/article/want-a-career-in-cybersecurity-here-	https://www.securitydegreehub.com/top-security-careers/	https://cybersecjobs.com/	https://www.securitywizardry.com/index.php/home/cnd-	http://resources.infosecinstitute.com/job-titles/#gref
Job Title	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
.NET Developer							x						
All Source-Collection Manager		x											
All Source-Collection Requirements Manager		x											
All-Source Analyst		x											
Application Developer							x						
Application Engineer	x						x						
Application Support Analyst							x						
Associate Developer							x						
Assurance Validator												x	
Authorizing Official/Designating Representative		x											
Business Continuity Manager													x
CHECK Team Leader												x	
Chief Information Officer	x						x						x
Chief Information Security Officer	x		x		x	x		x	x	x	x		x
Chief Security Officer	x					x					x		x
Chief Technology Officer (CTO)							x				x		
Cloud Architect							x						
Cloud Consultant							x						
Cloud Product and Project Manager							x						
Cloud Services Developer							x						
Cloud Software and Network Engineer							x						
Cloud System Administrator							x						
Cloud System Engineer							x						
Computer and Information Research Scientist							x						
Computer and Information Systems Manager							x						
Computer Forensics Expert									x				
Computer Forensics Investigator													x
Computer Network Architect							x						
Computer Programmer							x						
Computer Security Incident Responder			x		x								
Computer Security Incident Response Team Member												x	

A.3 Job Titles Color-Coded

Job Title
.NET Developer
All Source-Collection Manager
All Source-Collection Requirements Manager
All-Source Analyst
Application Developer
Application Engineer
Application Support Analyst
Associate Developer
Assurance Validator
Authorizing Official/Designating Representative
Business Continuity Manager
CHECK Team Leader
Chief Information Officer
Chief Information Security Officer
Chief Security Officer
Chief Technology Officer (CTO)
Cloud Architect
Cloud Consultant
Cloud Product and Project Manager
Cloud Services Developer
Cloud Software and Network Engineer
Cloud System Administrator
Cloud System Engineer
Computer and Information Research Scientist
Computer and Information Systems Manager
Computer Forensics Expert
Computer Forensics Investigator
Computer Network Architect
Computer Programmer
Computer Security Incident Responder
Computer Security Incident Response Team Member
Computer Systems Analyst
Computer Systems Manager
COMSEC Manager
Cross-Platform Security Architect
Cryptanalyst
Cryptographer/Cryptologist
Customer Support Administrator
Customer Support Specialist

Cyber Crime Investigator
Cyber Defense Analyst
Cyber Defense Forensics Analyst
Cyber Defense Incident Responder
Cyber Defense Infrastructure Support Specialist
Cyber Instructional Curriculum Developer
Cyber Instructor
Cyber Intel Planner
Cyber Legal Advisor
Cyber Operator
Cyber Ops Planner
Cyber Policy and Strategy Planner
Cyber Workforce Developer and Manager
Cybersecurity Lead
Data Administrator
Data Center Manager
Data Center Support Specialist
Data Protection Officer
Data Quality Manager
Data Recovery Specialist
Database Administrator
Desktop Support Manager
Desktop Support Specialist
Developer
Director of Security
Director of Technology
Disaster Recovery Specialist
Enterprise Architect
Executive Cyber Leadership
Exploitation Analyst
Forensic Analyst
Forensic Computer Analyst
Forensic Expert
Forensics Engineer
Front End Developer
Global Head of IT/Information Security
Global Information Security Director
Help Desk Specialist
Help Desk Technician
Incident Responder
Information Architect

Information Assurance Analyst
Information Assurance Engineer
Information Assurance Manager
Information Security Analyst
Information Security Architect
Information Security Auditor
Information Security Director
Information Security Engineer
Information Security Manager
Information Systems Auditor
Information Systems Security Developer
Information Systems Security Manager
Intrusion Detection Specialist
IT Analyst
IT Business Analyst
IT Coordinator
IT Director
IT Investment/Portfolio Manager
IT Manager
IT Program Auditor
IT Project Manager
IT Security Analyst
IT Security Consultant
IT Security Engineer
IT Support Specialist
IT Systems Administrator
Java Developer
Junior Software Engineer
Knowledge Manager
Lead Security Engineer
Lead Software Security Engineer
Malware Analyst
Management Information Systems Director
Mission Assessment Specialist
Multi-Disciplined Language Analyst
Network Administrator
Network and Computer Systems Administrator
Network Architect
Network Engineer
Network Operations Specialist
Network Security Administrator

Network Security Engineer
Network Systems Administrator
Partner Inegrations Planner
Penetration Tester (Ethical Hacker or Assurance Validator)
Privacy Complicance Manager
Privacy Officer
Product Support Manager
Program Analyst
Program Manager
Programmer
Research & Development Specialist
Risk Analyst
SCADA (Supervisory Control and Data Acquisition) Technician
Secure Software Assessor
Security Administrator
Security Analyst
Security Architect
Security Auditor
Security Code Auditor
Security Consultant
Security Control Assessor
Security Director
Security Engineer
Security Manager
Security Post-Sales Engineer
Security Pre-Sales Engineer
Security Researcher
Security Sales Account Manager
Security Software Developer
Security Specialist
Security Systems Administrator
Senior Application Engineer
Senior Data Systems Administrator
Senior IT Auditor
Senior Network Architect
Senior Network Engineer
Senior Network System Administrator
Senior Program Analyst
Senior Programmer
Senior Security Specialist
Senior Software Engineer

Senior Support Specialist
Senior System Designer
Senior Systems Administrator
Senior Systems Analyst
Senior Systems Architect
Senior Systems Software Engineer
Senior Web Administrator
Senior Web Developer
Software Architect
Software Developer
Software Engineer
Software Quality Assurance Analyst
Source Code Auditor
Support Specialist
System Testing and Evaluation Specialist
System, Network, and/or Web Penetration Tester
Systems Administrator
Systems Analyst
Systems Architect
Systems Designer
Systems Developer
Systems Requirements Planner
Systems Security Analyst
Systems Software Engineer
Target Developer
Target Network Analyst
Technical Operations Officer
Technical Specialist
Technical Support Engineer
Technical Support Specialist
Telecommunications Specialist
Virus Technician
Vulnerability Assessment Analyst
Vulnerability Assessor
Vulnerability Researcher
Warning Analyst
Web Administrator
Web Developer
Webmaster

A.4 Reduction and Codification Process

Chapter 04 Functions 00 - Reduction and Codification Process

[Chapter04_Functions_01.txt]
Step 01 - Overview
List Careers as reduced into Categories

[Chapter04_Functions_02.txt]
Step 2 - Codification

a) Remove Defensive and Offensive designations

Communication and Reporting
Cryptographic Implementation
Cryptography, Cryptanalysis, Blockchain
Data Privacy and Protection
Disaster Recovery and Continuity
Documentation and Cataloging
Forensics and Data Recovery
Information Classification
Intelligence Analysis
Intelligence Collection
Intrusion and Incident Analysis
Malware Analysis
Management and Coordination
Monitoring and Alerting
Planning and Design
Policy Creation and Administration
Policy, Legal, and Compliance Investigation
Project Management
Research and Analysis
Risk, Auditing, and Inventory
Secure Software Engineer
Security Training Design and Delivery
Social Engineering and Infiltration
System Implementation
Technical Investigation and Exploitation
Vulnerability Analysis

b) Expand combinatory functions and remove duplicates

(Example: "Research and Analysis" to "Research" "Analysis")

Alerting
Analysis
Auditing
Blockchain
Business Continuity
Cataloging
Communication
Coordination
Cryptanalysis
Cryptographic Implementation
Cryptography
Data Privacy
Data Protection
Data Recovery
Design
Disaster Recovery
Documentation
Forensics
Incident Analysis
Information Classification
Intelligence Analysis
Intelligence Collection
Intrusion Analysis
Inventory
Legal Compliance
Malware Analysis
Management
Monitoring
Physical Infiltration
Planning
Policy Administration
Policy Compliance
Policy Creation
Programming
Project Management
Reporting
Research
Risk Analysis
Social Engineering
System Implementation
Technical Exploitation
Technical Investigation
Training Delivery
Training Design
Vulnerability Analysis

```
┌─[ppoteete@z620foo]─[/tmp/functions]
└──□ $cat list| sort -k2
         Alerting
         Analysis
         Auditing
         Blockchain
         Cataloging
         Communication
         Coordination
```

```
    Cryptanalysis
    Cryptography
    Design
    Documentation
    Forensics
    Inventory
    Management
    Monitoring
    Planning
    Programming
    Reporting
    Research
    Policy Administration
    Incident Analysis
    Intelligence Analysis
    Intrusion Analysis
    Malware Analysis
    Risk Analysis
    Vulnerability Analysis
    Information Classification
    Intelligence Collection
    Legal Compliance
    Policy Compliance
    Business Continuity
    Policy Creation
    Training Delivery
    Training Design
    Social Engineering
    Technical Exploitation
    Cryptographic Implementation
    System Implementation
    Physical Infiltration
    Technical Investigation
    Project Management
    Data Privacy
    Data Protection
    Data Recovery
    Disaster Recovery
```

c) Determine distiguishing characteristics

```
┌──[ppoteete@z620foo]─[/tmp/functions]
└──⍰ $cat list | awk '{ print $1 }'| sort | uniq -
c | sort -n
      1 Alerting
      1 Analysis
      1 Auditing
      1 Blockchain
      1 Business
      1 Cataloging
      1 Communication
      1 Coordination
      1 Cryptanalysis
      1 Cryptographic
      1 Cryptography
      1 Design
      1 Disaster
      1 Documentation
      1 Forensics
      1 Incident
      1 Information
      1 Intrusion
      1 Inventory
      1 Legal
      1 Malware
      1 Management
      1 Monitoring
      1 Physical
      1 Planning
      1 Programming
      1 Project
      1 Reporting
      1 Research
      1 Risk
      1 Social
      1 System
      1 Vulnerability
      2 Intelligence
      2 Technical
      2 Training
      3 Data
      3 Policy
```

```
┌──[ppoteete@z620foo]─[/tmp/functions]
└──⍰ $cat list | awk '{ print $2 }'| sort | uniq -
c | sort -n
      1 Administration
      1 Classification
      1 Collection
      1 Continuity
      1 Creation
      1 Delivery
      1 Design
      1 Engineering
      1 Exploitation
      1 Infiltration
      1 Investigation
      1 Management
      1 Privacy
      1 Protection
      2 Compliance
      2 Implementation
      2 Recovery
      6 Analysis
```

d) Reduction based on procedural and functional characteristics

Example:
Procedural: Analysis, Coordination, Research
Functional: Blockchain, Compliance

```
┌─[ppoteete@z620foo]─[/tmp/functions]
└──▯ $for line in `cat list`; do echo $line;
done | sort | uniq | sort
Administration
Alerting
Analysis
Auditing
Blockchain
Business
Cataloging
Classification
Collection
Communication
Compliance
Continuity
Coordination
Creation
Cryptanalysis
Cryptographic
Cryptography
Data
Delivery
Design
Disaster
Documentation
Engineering
Exploitation
Forensics
Implementation
Incident
Infiltration
Information
Intelligence
Intrusion
Inventory
Investigation
Legal
Malware
Management
Monitoring
Physical
Planning
Policy
Privacy
Programming
Project
Protection
Recovery
Reporting
Research
Risk
Social
System
Technical
Training
Vulnerability
```


Procedural Codification:
Organizer:
- Administration
- Classification
- Collection

Creator:
- Design
- Engineering

Implementor:
- Delivery
- Implementation

- Exploitation
- Infiltration
- Recovery

Investigator:
- Investigation
- Analysis
- Compliance

Manager:
- Management

Protection

NOTE: These are not job titles, but job functions

Policy Creation and Administration
Management and Coordination
Communication and Reporting
Project Management
Risk, Auditing, and Inventory
Documentation and Cataloging
Information Classification
Data Privacy and Protection
Secure Software Engineer

```
Cryptography, Cryptanalysis, Blockchain
Intelligence Collection
Defense Monitoring and Alerting
Malware Analysis
System Implementation
Research and Analysis
Intrusion and Incident Analysis
Cryptographic Implementation
Forensics and Data Recovery
Disaster Recovery and Continuity
Intelligence Analysis
Security Training Design and Delivery
Planning and Design
Social Engineering and Infiltration
Technical Investigation and Exploitation
Offensive Research and Analysis
Policy, Legal, and Compliance Investigation
Vulnerability Analysis

┌─[ppoteete@z620foo]─[/tmp/functions]
└──╼ $cat list.2 | sort | uniq | sort -n
Communication and Reporting
Cryptographic Implementation
Data Privacy and Protection
Defense Monitoring and Alerting
Disaster Recovery and Continuity
Documentation and Cataloging
Forensics and Data Recovery
Intrusion and Incident Analysis
Malware Analysis
Management and Coordination
Planning and Design
Policy Creation and Administration
Legal and Compliance Investigation
Project Management
Research and Analysis
Secure Software Engineer
Security Training Design and Delivery
Social Engineering and Infiltration
System Implementation
Vulnerability Analysis
Technical Exploitation
Physical Infiltration

┌─[ppoteete@z620foo]─[/tmp/functions]
└──╼ $cat list.4 | sort
Communication and Reporting
Cryptographic Implementation
Data Privacy and Protection
Defense Monitoring and Alerting
Disaster Recovery and Continuity
Documentation and Cataloging
Forensics and Data Recovery
```

```
Intrusion and Incident Analysis
Legal and Compliance Investigation
Malware Analysis
Management and Coordination
Physical Infiltration
Planning and Design
Policy Creation and Administration
Project Management
Research and Analysis
Secure Software Engineering
Security Training Design and Delivery
Social Engineering and Infiltration
System Implementation
Technical Exploitation
Vulnerability Analysis

┌─[ppoteete@z620foo]─[/tmp/functions]
└──╼ $cat list.4 | sort | sed s/and\ //g | sort -k2
Malware Analysis
Research Analysis
Vulnerability Analysis
Documentation Cataloging
Legal Compliance Investigation
Management Coordination
Policy Creation Administration
Forensics Data Recovery
Planning Design
Social Engineering Infiltration
Technical Exploitation
Cryptographic Implementation
System Implementation
Intrusion Incident Analysis
Physical Infiltration
Project Management
Defense Monitoring Alerting
Data Privacy Protection
Disaster Recovery Continuity
Communication Reporting
Secure Software Engineer
Security Training Design Delivery

┌─[ppoteete@z620foo]─[/tmp/functions]
└──╼ $cat list.4 | sort | sed s/and\ /_/g | sort -
k2 | sed s/_/and\ /g
Malware Analysis
Vulnerability Analysis
Research and Analysis
Documentation and Cataloging
Legal and Compliance Investigation
Management and Coordination
Policy Creation and Administration
Data Forensics
Planning and Design
```

```
Social Engineering and Infiltration
Technical Exploitation
Cryptographic Implementation
System Implementation
Intrusion Analysis
Physical Infiltration
System Monitoring
Communication and Reporting
Secure Software Engineering
Security Training Design and Delivery

┌─[ppoteete@z620foo]─[/tmp/functions]
└──⍰ $cat list | grep -v and | sort -k2
Intrusion Analysis
Malware Analysis
Vulnerability Analysis
Technical Exploitation
Data Forensics
Technical Implementation
Physical Infiltration
System Monitoring
Secure Software Engineering

┌─[ppoteete@z620foo]─[/tmp/functions]
└──⍰ $cat list | grep and | sort -k3
Research and Development
Policy Creation and Administration
Social Engineering and Infiltration
Documentation and Cataloging
Legal and Compliance Investigation
Management and Coordination
Mission Planning
Security Training Design and Delivery
Communication and Reporting

┌─[ppoteete@z620foo]─[/tmp/functions]
└──⍰ $cat list | sort
Communication and Reporting
Data Forensics
Documentation and Cataloging
Intrusion Analysis
Legal and Compliance Investigation
Malware Analysis
Management and Coordination
Mission Planning
Physical Infiltration
Policy Creation and Administration
Research and Development
Secure Software Engineering
Security Training Design and Delivery
Social Engineering and Infiltration
System Monitoring
Technical Exploitation
Technical Implementation
Vulnerability Analysis
```

Operational:
Communication and Reporting
Documentation and Cataloging
Management and Coordination
Mission Planning
Policy Creation and Administration
System Monitoring
Technical Implementation
Research and Development
Secure Software Engineering

Defensive:
Data Forensics
Intrusion Analysis
Malware Analysis
Security Training Design
Security Training Delivery

Offensive:
Legal and Compliance Investigation
Physical Infiltration
Social Engineering and Infiltration
Technical Exploitation
Vulnerability Analysis

B.1 Informed Consent

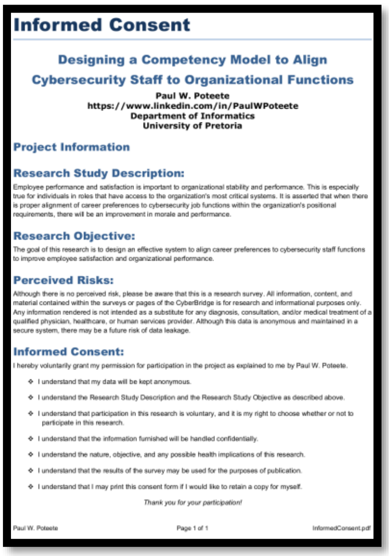
Paul W. Poteete

https://www.linkedin.com/in/PaulWPoteete

Department of Informatics

University of Pretoria

Project Information



Informed Consent

Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions

Paul W. Poteete
https://www.linkedin.com/in/PaulWPoteete
Department of Informatics
University of Pretoria

Project Information

Research Study Description:

Employee performance and satisfaction is important to organizational stability and performance. This is especially true for individuals in roles that have access to the organization's most critical systems. It is asserted that when there is proper alignment of career preferences to cybersecurity job functions within the organization's positional requirements, there will be an improvement in morale and performance.

Research Objective:

The goal of this research is to design an effective system to align career preferences to cybersecurity staff functions to improve employee satisfaction and organizational performance.

Perceived Risks:

Although there is no perceived risk, please be aware that this is a research survey. All information, content, and material contained within the surveys or pages of the CyberBridge is for research and informational purposes only. Any information rendered is not intended as a substitute for any diagnosis, consultation, and/or medical treatment of a qualified physician, healthcare, or human services provider. Although this data is anonymous and maintained in a secure system, there may be a future risk of data leakage.

Informed Consent:

I hereby voluntarily grant my permission for participation in the project as explained to me by Paul W. Poteete.

- I understand that my data will be kept anonymous.
- I understand the Research Study Description and the Research Study Objective as described above.
- I understand that participation in this research is voluntary, and it is my right to choose whether or not to participate in this research.
- I understand that the information furnished will be handled confidentially.
- I understand the nature, objective, and any possible health implications of this research.
- I understand that the results of the survey may be used for the purposes of publication.
- I understand that I may print this consent form if I would like to retain a copy for myself.

Thank you for your participation!

Paul W. Poteete Page 1 of 1 InformedConsent.pdf

Research Study Description:

Employee performance and satisfaction is important to organizational stability and performance. This is especially true for individuals in roles that have access to the organization's most critical systems. It is asserted that when there is proper alignment of career preferences to cybersecurity job functions within the organization's positional requirements, there will be an improvement in morale and performance.

Research Objective:

The goal of this research is to design an effective system to align career preferences to cybersecurity staff functions to improve employee satisfaction and organizational performance.

Perceived Risks:

Although there is no perceived risk, please be aware that this is a research survey. All information, content, and material contained within the surveys or pages of the CyberBridge is for research and informational purposes only.

Any information rendered is not intended as a substitute for any diagnosis, consultation, and/or medical treatment of a qualified physician, healthcare, or human services provider. Although this data is anonymous and maintained in a secure system, there may be a future risk of data leakage.

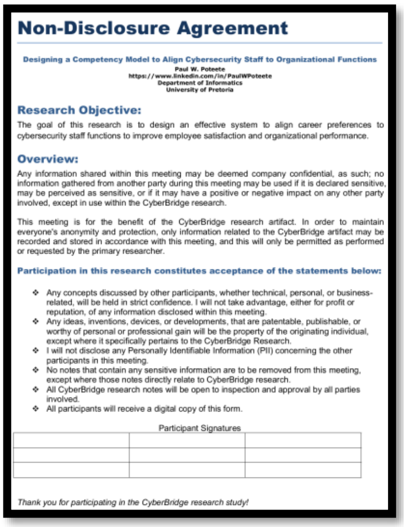
Informed Consent:

- I hereby voluntarily grant my permission for participation in the project as explained to me by Paul W. Poteete.

- I understand that my data will be kept anonymous.
- I understand the Research Study Description and the Research Study Objective as described above.
- I understand that participation in this research is voluntary, and it is my right to choose whether or not to participate in this research.
- I understand that the information furnished will be handled confidentially.
- I understand the nature, objective, and any possible health implications of this research.
- I understand that the results of the survey may be used for the purposes of publication.
- I understand that I may print this consent form if I would like to retain a copy for myself.

Thank you for your participation!

B.2 Non-Disclosure Agreement (NDA)



Non-Disclosure Agreement

Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions

Paul W. Poteete
https://www.linkedin.com/in/PaulWPoteete
Department of Informatics
University of Pretoria

Research Objective:

The goal of this research is to design an effective system to align career preferences to cybersecurity staff functions to improve employee satisfaction and organizational performance.

Overview:

Any information shared within this meeting may be deemed company confidential, as such; no information gathered from another party during this meeting may be used if it is declared sensitive, may be perceived as sensitive, or if it may have a positive or negative impact on any other party involved, except in use within the CyberBridge research.

This meeting is for the benefit of the CyberBridge research artifact. In order to maintain everyone's anonymity and protection, only information related to the CyberBridge artifact may be recorded and stored in accordance with this meeting, and this will only be permitted as performed or requested by the primary researcher.

Participation in this research constitutes acceptance of the statements below:

- Any concepts discussed by other participants, whether technical, personal, or business-related, will be held in strict confidence. I will not take advantage, either for profit or reputation, of any information disclosed within this meeting.
- Any ideas, inventions, devices, or developments, that are patentable, publishable, or worthy of personal or professional gain will be the property of the originating individual, except where it specifically pertains to the CyberBridge Research.
- I will not disclose any Personally Identifiable Information (PII) concerning the other participants in this meeting.
- No notes that contain any sensitive information are to be removed from this meeting, except where those notes directly relate to CyberBridge research.
- All CyberBridge research notes will be open to inspection and approval by all parties involved.
- All participants will receive a digital copy of this form.

Participant Signatures

Thank you for participating in the CyberBridge research study!

Paul W. Poteete

https://www.linkedin.com/in/PaulWPoteete

Department of Informatics

University of Pretoria

Research Objective:

The goal of this research is to design an effective system to align career preferences to cybersecurity staff functions to improve employee satisfaction and organizational performance.

Overview:

Any information shared within this meeting may be deemed company confidential, as such; no information gathered from another party during this meeting may be used if it is declared sensitive, may be perceived as sensitive, or if it may have a positive or negative impact on any other party involved, except in use within the CyberBridge research.

This meeting is for the benefit of the CyberBridge research artifact. In order to maintain everyone's anonymity and protection, only information related to the CyberBridge artifact may be recorded and stored in accordance with this meeting, and this will only be permitted as performed or requested by the primary researcher.

Participation in this research constitutes acceptance of the statements below:

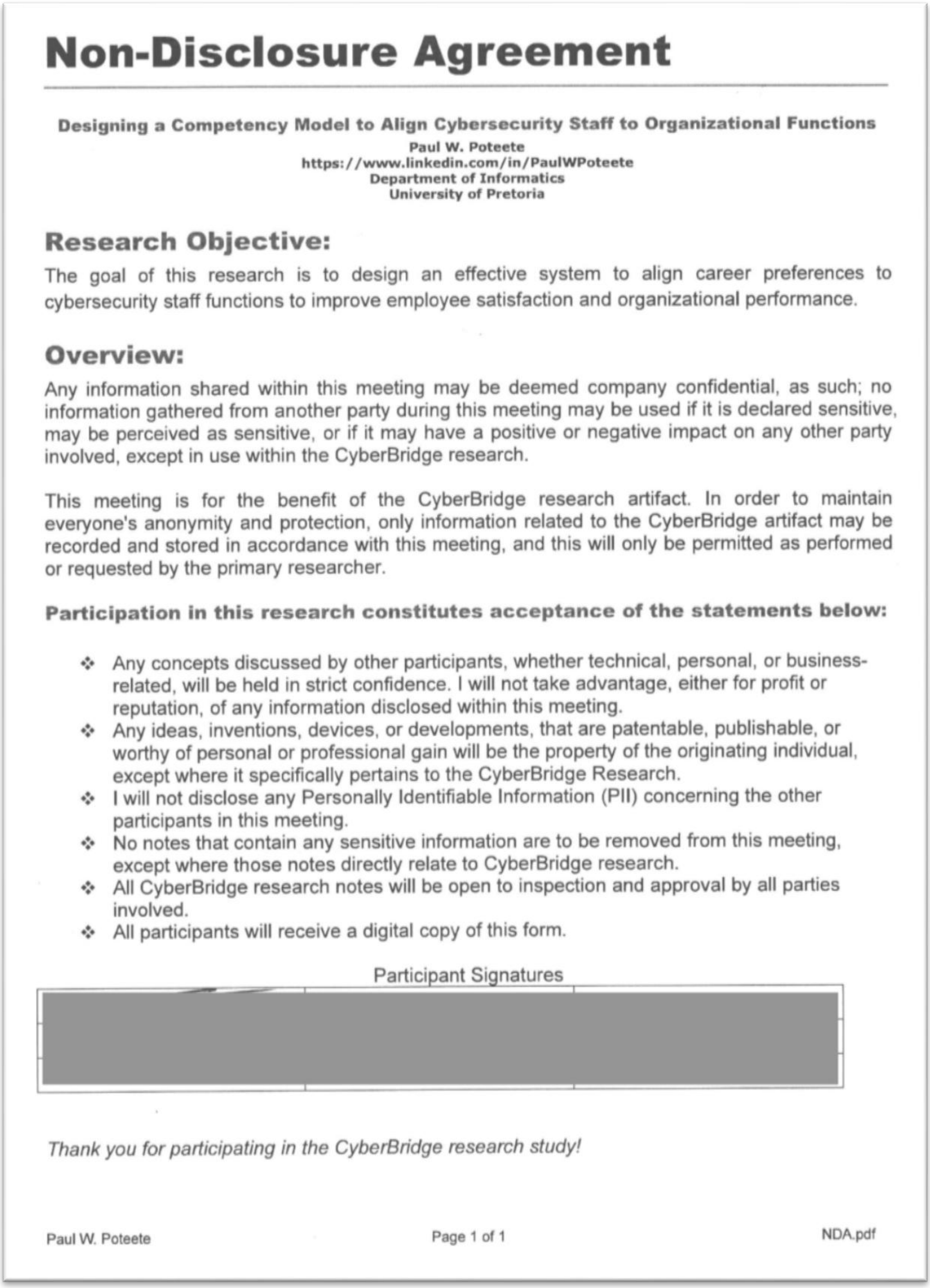
- Any concepts discussed by other participants, whether technical, personal, or business-related, will be held in strict confidence. I will not take advantage, either for profit or reputation, of any information disclosed within this meeting.
- Any ideas, inventions, devices, or developments, that are patentable, publishable, or worthy of personal or professional gain will be the property of the originating individual, except where it specifically pertains to the CyberBridge Research.
- I will not disclose any Personally Identifiable Information (PII) concerning the other participants in this meeting.
- No notes that contain any sensitive information are to be removed from this meeting, except where those notes directly relate to CyberBridge research.

- All CyberBridge research notes will be open to inspection and approval by all parties involved.
- All participants will receive a digital copy of this form.

Participant Signatures

Thank you for participating in the CyberBridge research study!

B.2 Non-Disclosure Agreement (NDA)



Non-Disclosure Agreement

Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions

Paul W. Poteete
https://www.linkedin.com/in/PaulWPoteete
Department of Informatics
University of Pretoria

Research Objective:

The goal of this research is to design an effective system to align career preferences to cybersecurity staff functions to improve employee satisfaction and organizational performance.

Overview:

Any information shared within this meeting may be deemed company confidential, as such; no information gathered from another party during this meeting may be used if it is declared sensitive, may be perceived as sensitive, or if it may have a positive or negative impact on any other party involved, except in use within the CyberBridge research.

This meeting is for the benefit of the CyberBridge research artifact. In order to maintain everyone's anonymity and protection, only information related to the CyberBridge artifact may be recorded and stored in accordance with this meeting, and this will only be permitted as performed or requested by the primary researcher.

Participation in this research constitutes acceptance of the statements below:

- Any concepts discussed by other participants, whether technical, personal, or business-related, will be held in strict confidence. I will not take advantage, either for profit or reputation, of any information disclosed within this meeting.
- Any ideas, inventions, devices, or developments, that are patentable, publishable, or worthy of personal or professional gain will be the property of the originating individual, except where it specifically pertains to the CyberBridge Research.
- I will not disclose any Personally Identifiable Information (PII) concerning the other participants in this meeting.
- No notes that contain any sensitive information are to be removed from this meeting, except where those notes directly relate to CyberBridge research.
- All CyberBridge research notes will be open to inspection and approval by all parties involved.
- All participants will receive a digital copy of this form.

Participant Signatures

[redacted]

Thank you for participating in the CyberBridge research study!

Paul W. Poteete   Page 1 of 1   NDA.pdf

B.3 Company Permission Letter

Paul W. Poteete

Primary Researcher

University of Pretoria

+1 412-626-2091

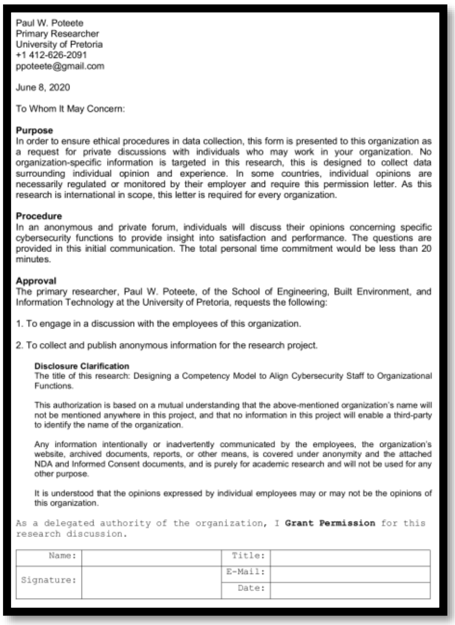
ppoteete@gmail.com

June 8, 2020

To Whom It May Concern:

Purpose

In order to ensure ethical procedures in data collection, this form is presented to this organization as a request for private discussions with individuals who may work in your organization. No organization-specific information is targeted in this research, this is designed to collect data surrounding individual opinion and experience. In some countries, individual opinions are necessarily regulated or monitored by their employer and require this permission letter. As this research is international in scope, this letter is required for every organization.



Paul W. Poteete
Primary Researcher
University of Pretoria
+1 412-626-2091
ppoteete@gmail.com

June 8, 2020

To Whom It May Concern:

Purpose
In order to ensure ethical procedures in data collection, this form is presented to this organization as a request for private discussions with individuals who may work in your organization. No organization-specific information is targeted in this research, this is designed to collect data surrounding individual opinion and experience. In some countries, individual opinions are necessarily regulated or monitored by their employer and require this permission letter. As this research is international in scope, this letter is required for every organization.

Procedure
In an anonymous and private forum, individuals will discuss their opinions concerning specific cybersecurity functions to provide insight into satisfaction and performance. The questions are provided in this initial communication. The total personal time commitment would be less than 20 minutes.

Approval
The primary researcher, Paul W. Poteete, of the School of Engineering, Built Environment, and Information Technology at the University of Pretoria, requests the following:

1. To engage in a discussion with the employees of this organization.

2. To collect and publish anonymous information for the research project.

Disclosure Clarification
The title of this research: Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions.

This authorization is based on a mutual understanding that the above-mentioned organization's name will not be mentioned anywhere in this project, and that no information in this project will enable a third-party to identify the name of the organization.

Any information intentionally or inadvertently communicated by the employees, the organization's website, archived documents, reports, or other means, is covered under anonymity and the attached NDA and Informed Consent documents, and is purely for academic research and will not be used for any other purpose.

It is understood that the opinions expressed by individual employees may or may not be the opinions of this organization.

As a delegated authority of the organization, I **Grant Permission** for this research discussion.

Name:		Title:	
Signature:		E-Mail:	
		Date:	

Procedure

In an anonymous and private forum, individuals will discuss their opinions concerning specific cybersecurity functions to provide insight into satisfaction and performance. The questions are provided in this initial communication. The total personal time commitment would be less than 20 minutes.

Approval

The primary researcher, Paul W. Poteete, of the School of Engineering, Built Environment, and Information Technology at the University of Pretoria, requests the following:

1. To engage in a discussion with the employees of this organization.

2. To collect and publish anonymous information for the research project.

Disclosure Clarification

The title of this research: Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions. This authorization is based on a mutual understanding that the above-mentioned organization's name will not be mentioned anywhere in this project, and that no information in this project will enable a third-party to identify the name of the organization. Any information intentionally or inadvertently communicated by the employees, the organization's website, archived documents, reports, or other means, is covered under anonymity and the attached NDA and Informed Consent documents, and is purely for academic research and will not be used for any other purpose. It is understood that the opinions expressed by individual employees may or may not be the opinions of this organization. As a delegated authority of the organization, I Grant Permission for this research discussion.

Name:

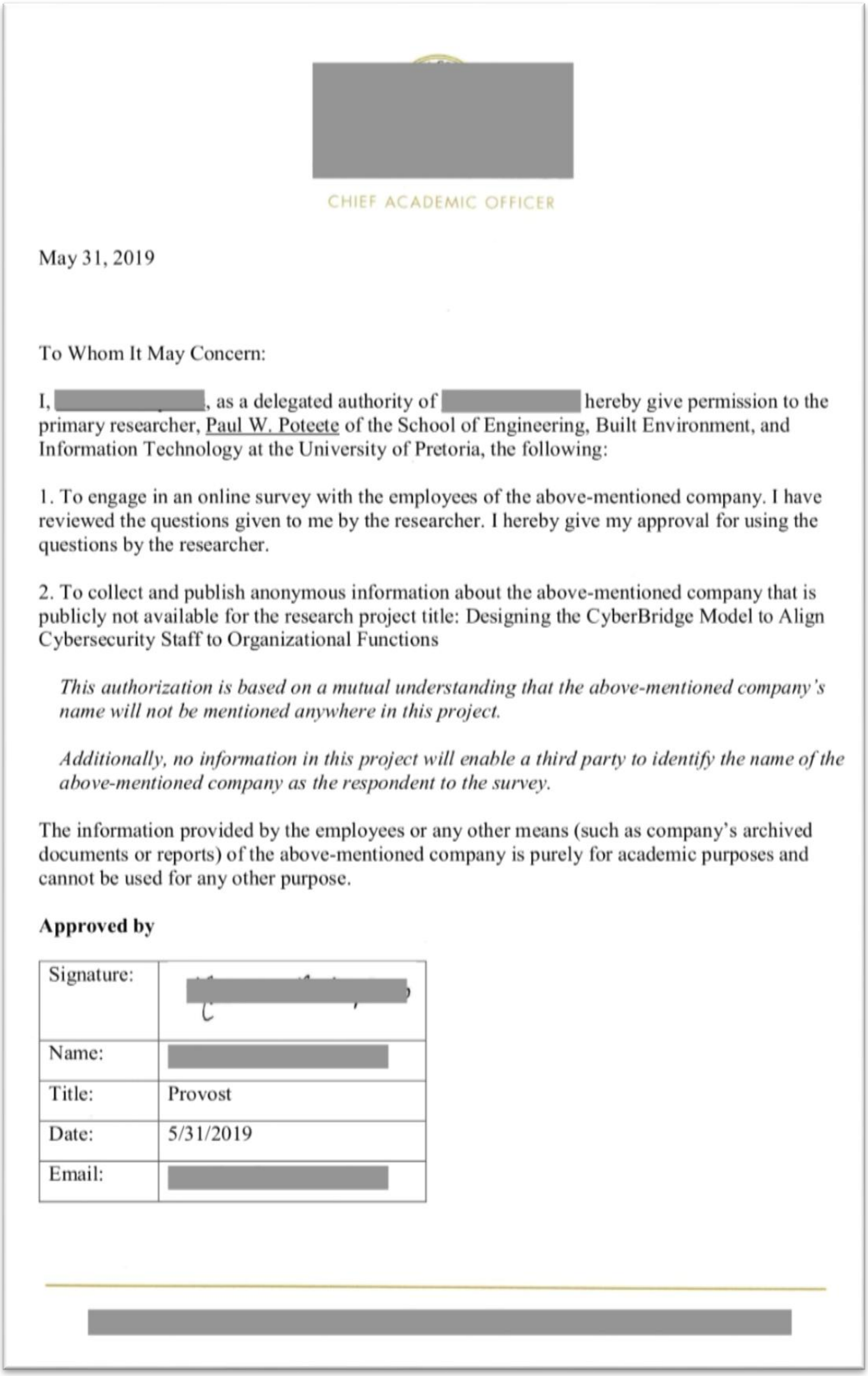
Signature:

Title:

E-Mail:

Date:

B.3 Company Permission Letter



[redacted]

CHIEF ACADEMIC OFFICER

May 31, 2019

To Whom It May Concern:

I, [redacted], as a delegated authority of [redacted] hereby give permission to the primary researcher, Paul W. Poteete of the School of Engineering, Built Environment, and Information Technology at the University of Pretoria, the following:

1. To engage in an online survey with the employees of the above-mentioned company. I have reviewed the questions given to me by the researcher. I hereby give my approval for using the questions by the researcher.

2. To collect and publish anonymous information about the above-mentioned company that is publicly not available for the research project title: Designing the CyberBridge Model to Align Cybersecurity Staff to Organizational Functions

> *This authorization is based on a mutual understanding that the above-mentioned company's name will not be mentioned anywhere in this project.*
>
> *Additionally, no information in this project will enable a third party to identify the name of the above-mentioned company as the respondent to the survey.*

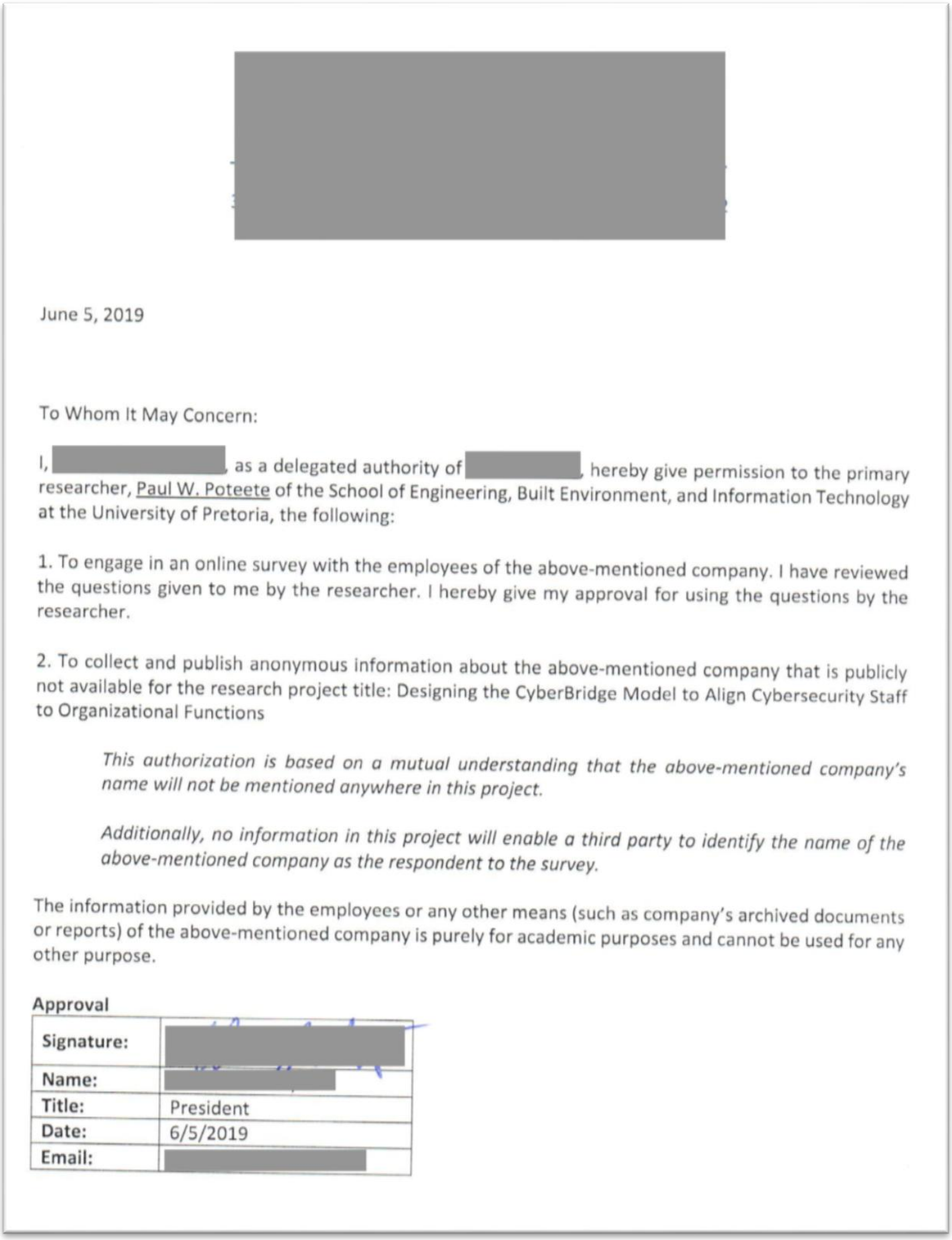
The information provided by the employees or any other means (such as company's archived documents or reports) of the above-mentioned company is purely for academic purposes and cannot be used for any other purpose.

Approved by

Signature:	[redacted]
Name:	[redacted]
Title:	Provost
Date:	5/31/2019
Email:	[redacted]

[redacted]

B.3 Company Permission Letters



[redacted]

June 5, 2019

To Whom It May Concern:

I, [redacted], as a delegated authority of [redacted], hereby give permission to the primary researcher, Paul W. Poteete of the School of Engineering, Built Environment, and Information Technology at the University of Pretoria, the following:

1. To engage in an online survey with the employees of the above-mentioned company. I have reviewed the questions given to me by the researcher. I hereby give my approval for using the questions by the researcher.

2. To collect and publish anonymous information about the above-mentioned company that is publicly not available for the research project title: Designing the CyberBridge Model to Align Cybersecurity Staff to Organizational Functions

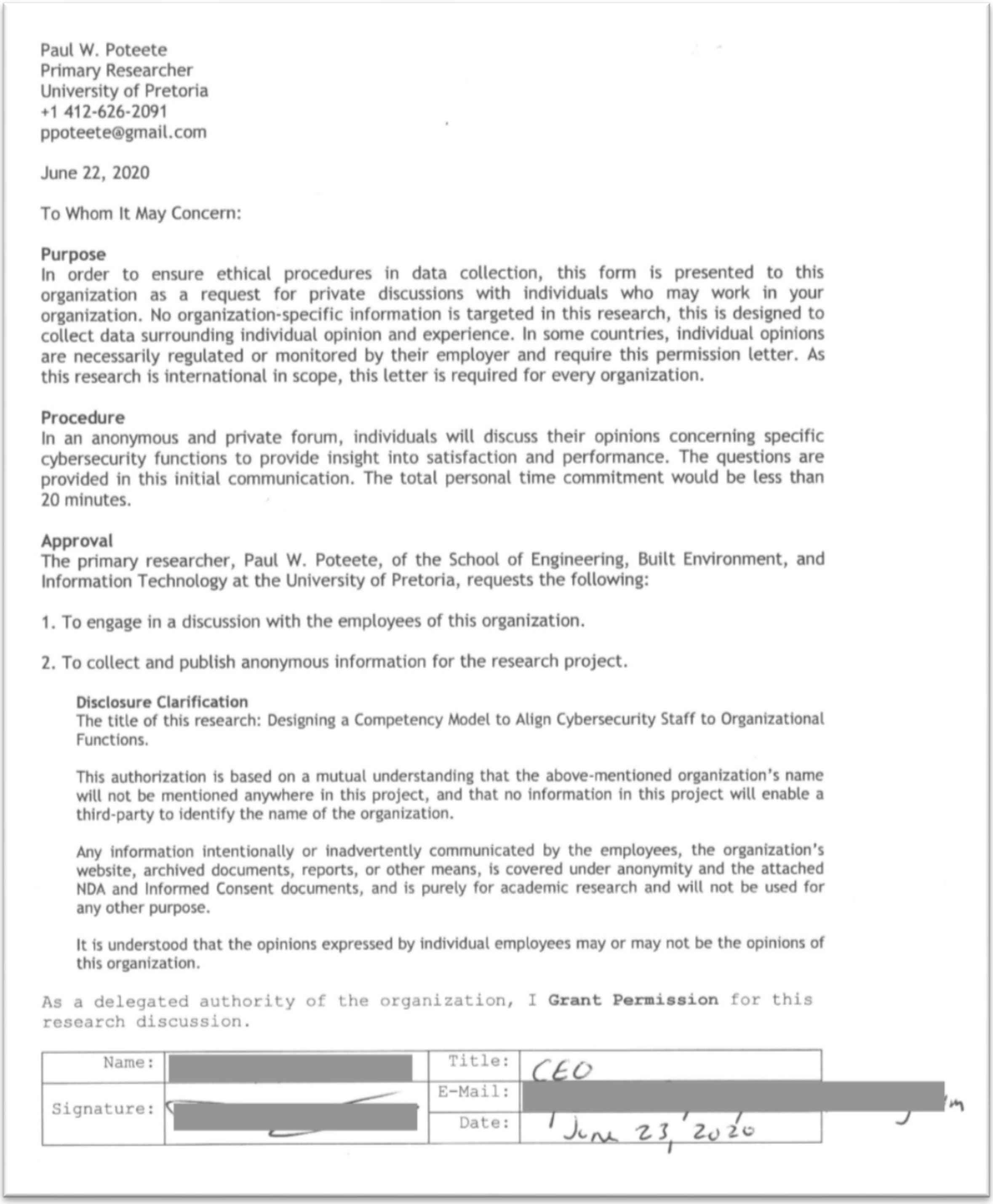
> *This authorization is based on a mutual understanding that the above-mentioned company's name will not be mentioned anywhere in this project.*
>
> *Additionally, no information in this project will enable a third party to identify the name of the above-mentioned company as the respondent to the survey.*

The information provided by the employees or any other means (such as company's archived documents or reports) of the above-mentioned company is purely for academic purposes and cannot be used for any other purpose.

Approval

Signature:	[redacted]
Name:	[redacted]
Title:	President
Date:	6/5/2019
Email:	[redacted]

B.3 Company Permission Letters



Paul W. Poteete
Primary Researcher
University of Pretoria
+1 412-626-2091
ppoteete@gmail.com

June 22, 2020

To Whom It May Concern:

Purpose
In order to ensure ethical procedures in data collection, this form is presented to this organization as a request for private discussions with individuals who may work in your organization. No organization-specific information is targeted in this research, this is designed to collect data surrounding individual opinion and experience. In some countries, individual opinions are necessarily regulated or monitored by their employer and require this permission letter. As this research is international in scope, this letter is required for every organization.

Procedure
In an anonymous and private forum, individuals will discuss their opinions concerning specific cybersecurity functions to provide insight into satisfaction and performance. The questions are provided in this initial communication. The total personal time commitment would be less than 20 minutes.

Approval
The primary researcher, Paul W. Poteete, of the School of Engineering, Built Environment, and Information Technology at the University of Pretoria, requests the following:

1. To engage in a discussion with the employees of this organization.

2. To collect and publish anonymous information for the research project.

Disclosure Clarification
The title of this research: Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions.

This authorization is based on a mutual understanding that the above-mentioned organization's name will not be mentioned anywhere in this project, and that no information in this project will enable a third-party to identify the name of the organization.

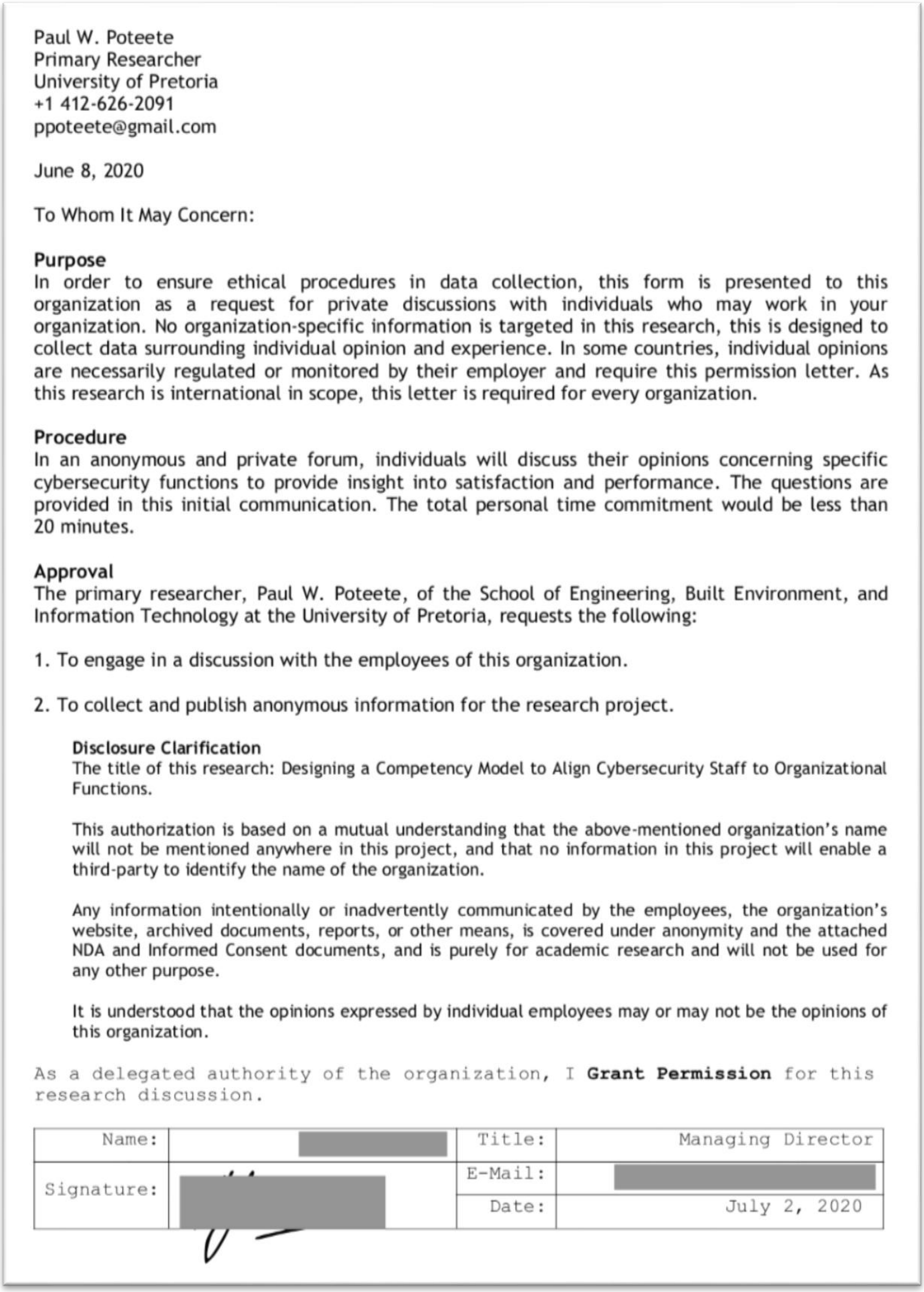
Any information intentionally or inadvertently communicated by the employees, the organization's website, archived documents, reports, or other means, is covered under anonymity and the attached NDA and Informed Consent documents, and is purely for academic research and will not be used for any other purpose.

It is understood that the opinions expressed by individual employees may or may not be the opinions of this organization.

As a delegated authority of the organization, I **Grant Permission** for this research discussion.

Name:	[redacted]	Title:	CEO
Signature:	[redacted]	E-Mail:	[redacted]
		Date:	June 23, 2020

B.3 Company Permission Letter



Paul W. Poteete
Primary Researcher
University of Pretoria
+1 412-626-2091
ppoteete@gmail.com

June 8, 2020

To Whom It May Concern:

Purpose
In order to ensure ethical procedures in data collection, this form is presented to this organization as a request for private discussions with individuals who may work in your organization. No organization-specific information is targeted in this research, this is designed to collect data surrounding individual opinion and experience. In some countries, individual opinions are necessarily regulated or monitored by their employer and require this permission letter. As this research is international in scope, this letter is required for every organization.

Procedure
In an anonymous and private forum, individuals will discuss their opinions concerning specific cybersecurity functions to provide insight into satisfaction and performance. The questions are provided in this initial communication. The total personal time commitment would be less than 20 minutes.

Approval
The primary researcher, Paul W. Poteete, of the School of Engineering, Built Environment, and Information Technology at the University of Pretoria, requests the following:

1. To engage in a discussion with the employees of this organization.

2. To collect and publish anonymous information for the research project.

Disclosure Clarification
The title of this research: Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions.

This authorization is based on a mutual understanding that the above-mentioned organization's name will not be mentioned anywhere in this project, and that no information in this project will enable a third-party to identify the name of the organization.

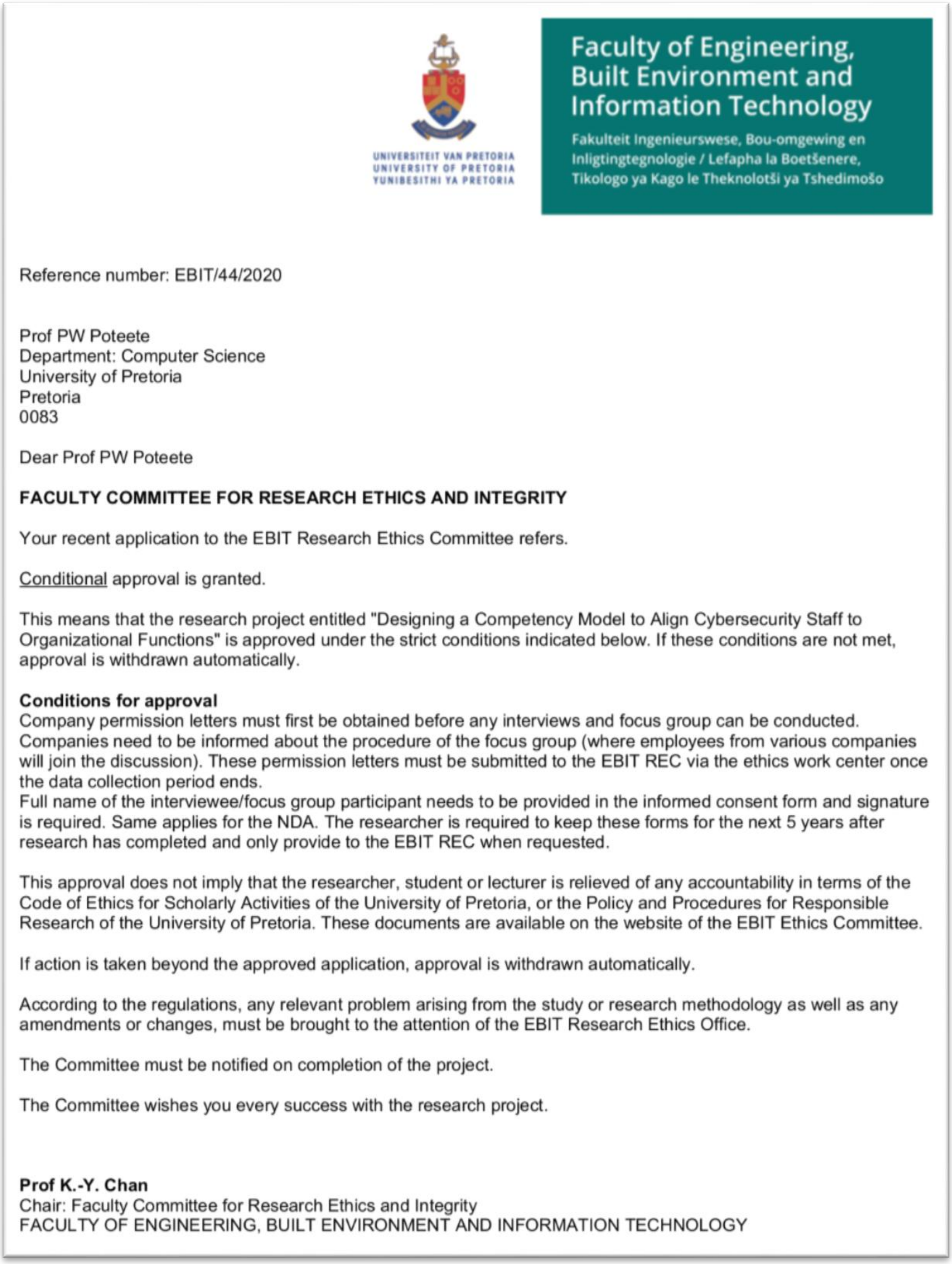
Any information intentionally or inadvertently communicated by the employees, the organization's website, archived documents, reports, or other means, is covered under anonymity and the attached NDA and Informed Consent documents, and is purely for academic research and will not be used for any other purpose.

It is understood that the opinions expressed by individual employees may or may not be the opinions of this organization.

As a delegated authority of the organization, I **Grant Permission** for this research discussion.

Name:	[redacted]	Title:	Managing Director
Signature:	[redacted]	E-Mail:	[redacted]
		Date:	July 2, 2020

B.4 Ethics Approval Letter



UNIVERSITEIT VAN PRETORIA
UNIVERSITY OF PRETORIA
YUNIBESITHI YA PRETORIA

Faculty of Engineering, Built Environment and Information Technology

Fakulteit Ingenieurswese, Bou-omgewing en Inligtingtegnologie / Lefapha la Boetšenere, Tikologo ya Kago le Theknolotši ya Tshedimošo

Reference number: EBIT/44/2020

Prof PW Poteete
Department: Computer Science
University of Pretoria
Pretoria
0083

Dear Prof PW Poteete

FACULTY COMMITTEE FOR RESEARCH ETHICS AND INTEGRITY

Your recent application to the EBIT Research Ethics Committee refers.

Conditional approval is granted.

This means that the research project entitled "Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions" is approved under the strict conditions indicated below. If these conditions are not met, approval is withdrawn automatically.

Conditions for approval
Company permission letters must first be obtained before any interviews and focus group can be conducted. Companies need to be informed about the procedure of the focus group (where employees from various companies will join the discussion). These permission letters must be submitted to the EBIT REC via the ethics work center once the data collection period ends.
Full name of the interviewee/focus group participant needs to be provided in the informed consent form and signature is required. Same applies for the NDA. The researcher is required to keep these forms for the next 5 years after research has completed and only provide to the EBIT REC when requested.

This approval does not imply that the researcher, student or lecturer is relieved of any accountability in terms of the Code of Ethics for Scholarly Activities of the University of Pretoria, or the Policy and Procedures for Responsible Research of the University of Pretoria. These documents are available on the website of the EBIT Ethics Committee.

If action is taken beyond the approved application, approval is withdrawn automatically.

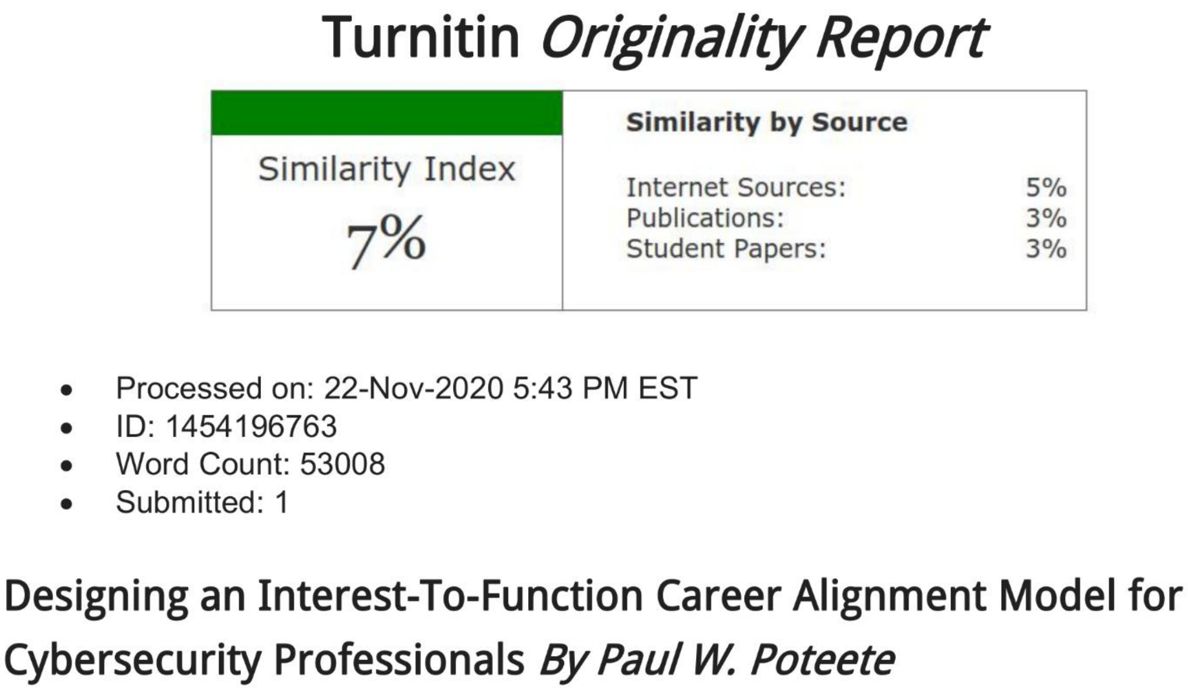
According to the regulations, any relevant problem arising from the study or research methodology as well as any amendments or changes, must be brought to the attention of the EBIT Research Ethics Office.

The Committee must be notified on completion of the project.

The Committee wishes you every success with the research project.

Prof K.-Y. Chan
Chair: Faculty Committee for Research Ethics and Integrity
FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION TECHNOLOGY

B.5 Turn It In Report



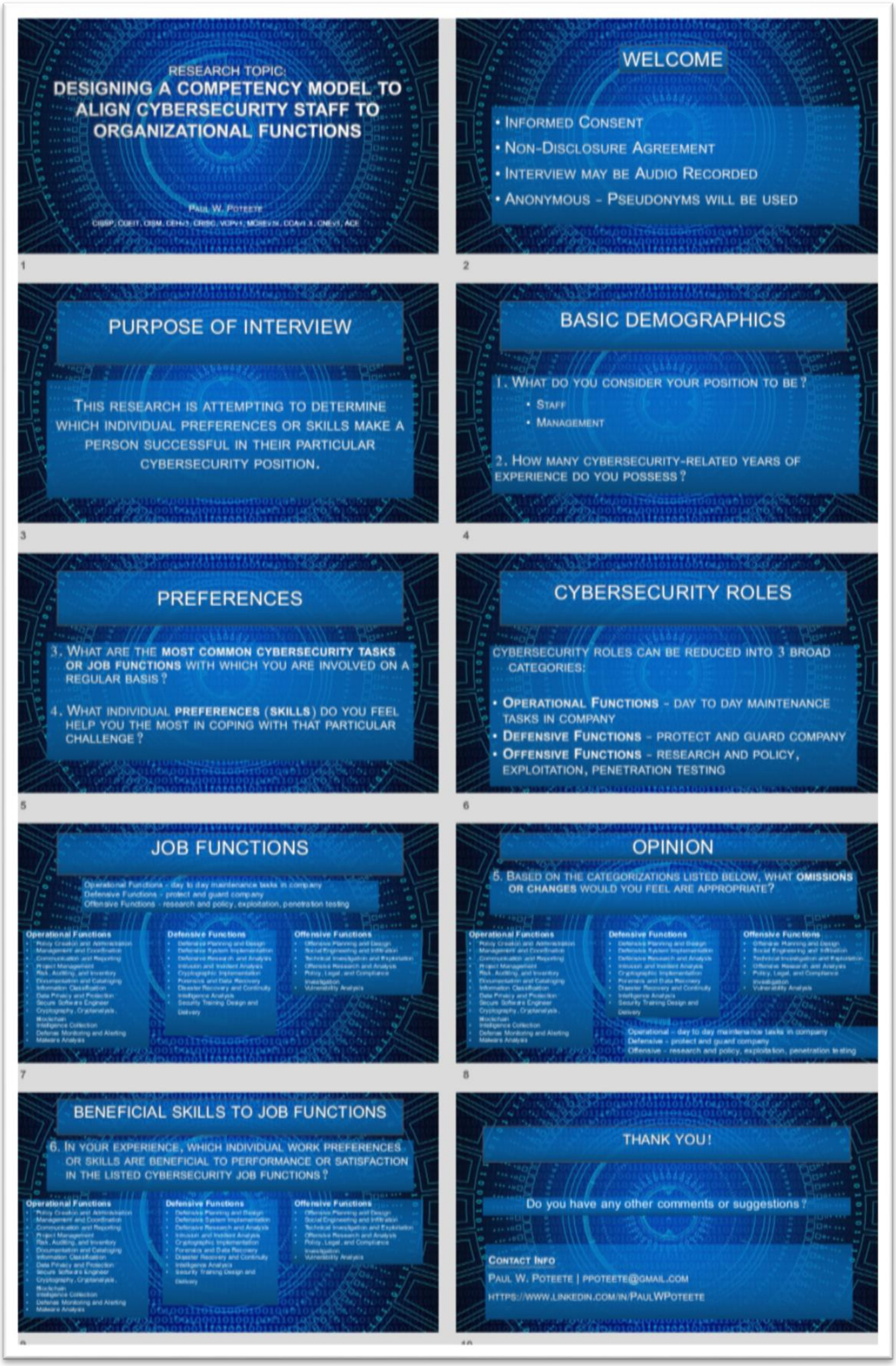
Turnitin *Originality Report*

Similarity Index	Similarity by Source	
7%	Internet Sources:	5%
	Publications:	3%
	Student Papers:	3%

- Processed on: 22-Nov-2020 5:43 PM EST
- ID: 1454196763
- Word Count: 53008
- Submitted: 1

Designing an Interest-To-Function Career Alignment Model for Cybersecurity Professionals *By Paul W. Poteete*

C.1 Interview Slides



RESEARCH TOPIC:

DESIGNING A COMPETENCY MODEL TO ALIGN CYBERSECURITY STAFF TO ORGANIZATIONAL FUNCTIONS

PAUL W. POTEETE

CISSP, CGEIT, CISM, CEHv3, CRISC, VCPv1, MCSEv.x, CCAv1.x, CNEv1, ACE

1

WELCOME

- INFORMED CONSENT
- NON-DISCLOSURE AGREEMENT
- INTERVIEW MAY BE AUDIO RECORDED
- ANONYMOUS - PSEUDONYMS WILL BE USED

2

PURPOSE OF INTERVIEW

THIS RESEARCH IS ATTEMPTING TO DETERMINE WHICH INDIVIDUAL PREFERENCES OR SKILLS MAKE A PERSON SUCCESSFUL IN THEIR PARTICULAR CYBERSECURITY POSITION.

3

BASIC DEMOGRAPHICS

1. WHAT DO YOU CONSIDER YOUR POSITION TO BE?
   - STAFF
   - MANAGEMENT
2. HOW MANY CYBERSECURITY-RELATED YEARS OF EXPERIENCE DO YOU POSSESS?

4

PREFERENCES

3. WHAT ARE THE **MOST COMMON CYBERSECURITY TASKS OR JOB FUNCTIONS** WITH WHICH YOU ARE INVOLVED ON A REGULAR BASIS?
4. WHAT INDIVIDUAL **PREFERENCES (SKILLS)** DO YOU FEEL HELP YOU THE MOST IN COPING WITH THAT PARTICULAR CHALLENGE?

5

CYBERSECURITY ROLES

CYBERSECURITY ROLES CAN BE REDUCED INTO 3 BROAD CATEGORIES:

- **OPERATIONAL FUNCTIONS** - DAY TO DAY MAINTENANCE TASKS IN COMPANY
- **DEFENSIVE FUNCTIONS** - PROTECT AND GUARD COMPANY
- **OFFENSIVE FUNCTIONS** - RESEARCH AND POLICY, EXPLOITATION, PENETRATION TESTING

6

JOB FUNCTIONS

Operational Functions - day to day maintenance tasks in company
Defensive Functions - protect and guard company
Offensive Functions - research and policy, exploitation, penetration testing

Operational Functions
- Policy Creation and Administration
- Management and Coordination
- Communication and Reporting
- Project Management
- Risk, Auditing, and Inventory
- Documentation and Cataloging
- Information Classification
- Data Privacy and Protection
- Secure Software Engineer
- Cryptography, Cryptanalysis, Blockchain
- Intelligence Collection
- Defense Monitoring and Alerting
- Malware Analysis

Defensive Functions
- Defensive Planning and Design
- Defensive System Implementation
- Defensive Research and Analysis
- Intrusion and Incident Analysis
- Cryptographic Implementation
- Forensics and Data Recovery
- Disaster Recovery and Continuity
- Intelligence Analysis
- Security Training Design and Delivery

Offensive Functions
- Offensive Planning and Design
- Social Engineering and Infiltration
- Technical Investigation and Exploitation
- Offensive Research and Analysis
- Policy, Legal, and Compliance Investigation
- Vulnerability Analysis

7

OPINION

5. BASED ON THE CATEGORIZATIONS LISTED BELOW, WHAT **OMISSIONS OR CHANGES** WOULD YOU FEEL ARE APPROPRIATE?

Operational Functions
- Policy Creation and Administration
- Management and Coordination
- Communication and Reporting
- Project Management
- Risk, Auditing, and Inventory
- Documentation and Cataloging
- Information Classification
- Data Privacy and Protection
- Secure Software Engineer
- Cryptography, Cryptanalysis, Blockchain
- Intelligence Collection
- Defense Monitoring and Alerting
- Malware Analysis

Defensive Functions
- Defensive Planning and Design
- Defensive System Implementation
- Defensive Research and Analysis
- Intrusion and Incident Analysis
- Cryptographic Implementation
- Forensics and Data Recovery
- Disaster Recovery and Continuity
- Intelligence Analysis
- Security Training Design and Delivery

Offensive Functions
- Offensive Planning and Design
- Social Engineering and Infiltration
- Technical Investigation and Exploitation
- Offensive Research and Analysis
- Policy, Legal, and Compliance Investigation
- Vulnerability Analysis

Operational - day to day maintenance tasks in company
Defensive - protect and guard company
Offensive - research and policy, exploitation, penetration testing

8

BENEFICIAL SKILLS TO JOB FUNCTIONS

6. IN YOUR EXPERIENCE, WHICH INDIVIDUAL WORK PREFERENCES OR SKILLS ARE BENEFICIAL TO PERFORMANCE OR SATISFACTION IN THE LISTED CYBERSECURITY JOB FUNCTIONS?

Operational Functions
- Policy Creation and Administration
- Management and Coordination
- Communication and Reporting
- Project Management
- Risk, Auditing, and Inventory
- Documentation and Cataloging
- Information Classification
- Data Privacy and Protection
- Secure Software Engineer
- Cryptography, Cryptanalysis, Blockchain
- Intelligence Collection
- Defense Monitoring and Alerting
- Malware Analysis

Defensive Functions
- Defensive Planning and Design
- Defensive System Implementation
- Defensive Research and Analysis
- Intrusion and Incident Analysis
- Cryptographic Implementation
- Forensics and Data Recovery
- Disaster Recovery and Continuity
- Intelligence Analysis
- Security Training Design and Delivery

Offensive Functions
- Offensive Planning and Design
- Social Engineering and Infiltration
- Technical Investigation and Exploitation
- Offensive Research and Analysis
- Policy, Legal, and Compliance Investigation
- Vulnerability Analysis

9

THANK YOU!

Do you have any other comments or suggestions?

CONTACT INFO

PAUL W. POTEETE | PPOTEETE@GMAIL.COM

HTTPS://WWW.LINKEDIN.COM/IN/PAULWPOTEETE

10

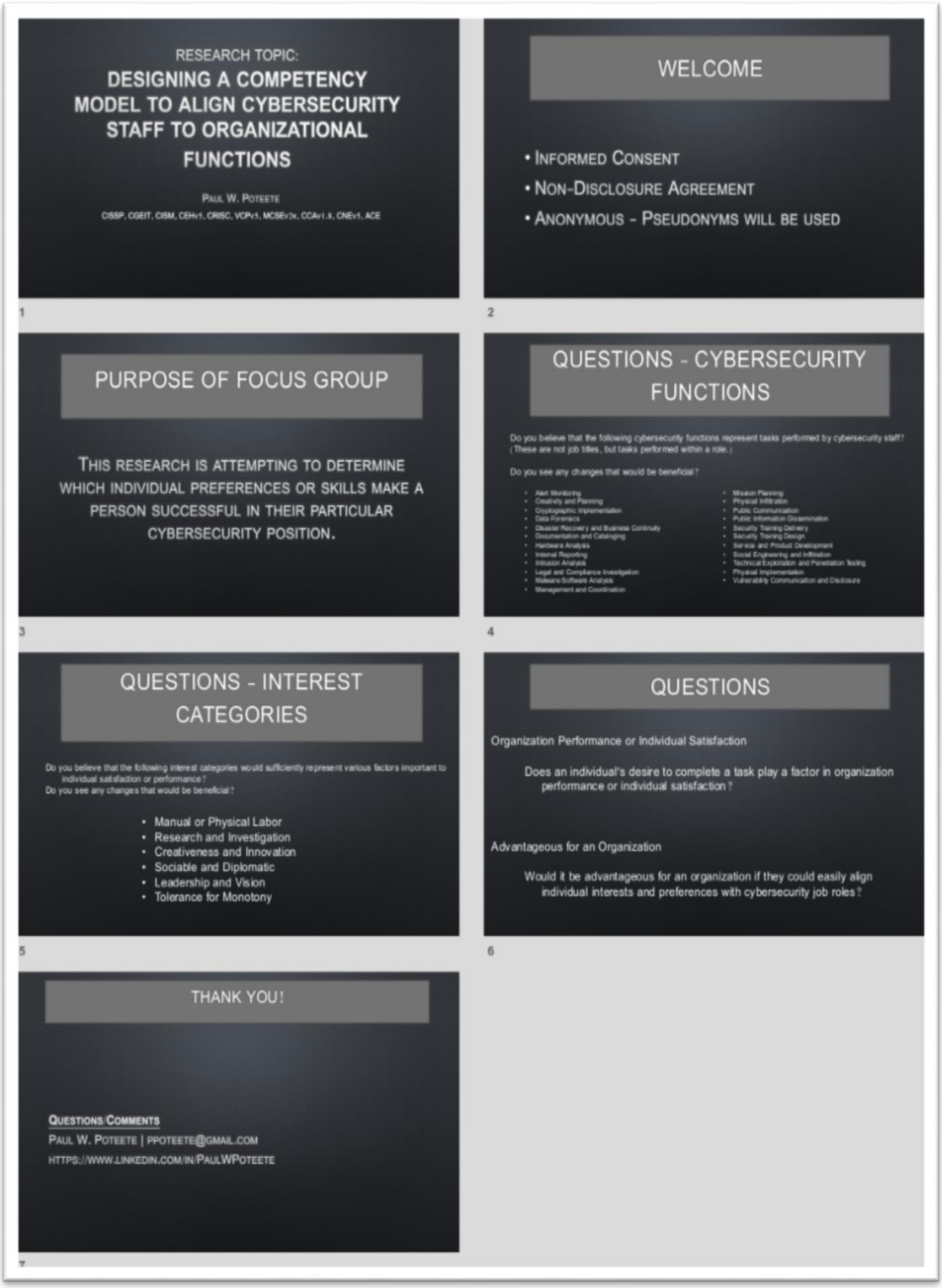
C.1 Interview Slides

Slide	Content
Slide 1	**Research Topic: Designing an Interest-to-Function Career Alignment Model for Cybersecurity Professionals** Paul W. Poteete CISSP, CGEIT, CISM, CEHv5, CRISC, VCPv5, MCSEv2k, CCAv1.8, CNEv5, ACE
Slide 2	**Welcome** • Informed Consent • Non-Disclosure Agreement • Interview may be Audio Recorded • Anonymous - Pseudonyms will be used
Slide 3	**Purpose of Interview** This research is attempting to determine which individual preferences or skills make a person successful in their particular cybersecurity position.
Slide 4	**Basic Demographics** 1. What do you consider your position to be? Staff Management 2. How many cybersecurity-related years of experience do you possess?
Slide 5	**Preferences** 3. What are the most common cybersecurity tasks or job functions with which you are involved on a regular basis? 4. What individual preferences (skills) do you feel help you the most in coping with that particular challenge?
Slide 6	**Cybersecurity Roles** Cybersecurity roles can be reduced into 3 broad categories: • Operational Functions - day to day maintenance tasks in company • Defensive Functions - protect and guard company • Offensive Functions - research and policy, exploitation, penetration testing

Slide	Content
Slide 7	**Job Functions** Operational Functions • Policy Creation and Administration • Management and Coordination • Communication and Reporting • Project Management • Risk, Auditing, and Inventory • Documentation and Cataloging • Information Classification • Data Privacy and Protection • Secure Software Engineer • Cryptography, Cryptanalysis, Blockchain • Intelligence Collection • Defense Monitoring and Alerting • Malware Analysis Defensive Functions • Defensive Planning and Design • Defensive System Implementation • Defensive Research and Analysis • Intrusion and Incident Analysis • Cryptographic Implementation • Forensics and Data Recovery • Disaster Recovery and Continuity • Intelligence Analysis • Security Training Design and Delivery Offensive Functions • Offensive Planning and Design • Social Engineering and Infiltration • Technical Investigation and Exploitation • Offensive Research and Analysis • Policy, Legal, and Compliance Investigation • Vulnerability Analysis
Slide 8	**Opinion** 5. Based on the categorizations listed below, what omissions or changes would you feel are appropriate? (Job Functions and Categories listed)
Slide 9	**Beneficial Skills to Job Functions**

Slide	Content
	6. In your experience, which individual work preferences or skills are beneficial to performance or satisfaction in the listed cybersecurity job functions?
Slide 10	**Thank you!** Do you have any other comments or suggestions? Contact Info Paul W. Poteete ppoteete@gmail.com https://www.linkedin.com/in/PaulWPoteete

C.2 Focus Group Slides



RESEARCH TOPIC:

DESIGNING A COMPETENCY MODEL TO ALIGN CYBERSECURITY STAFF TO ORGANIZATIONAL FUNCTIONS

PAUL W. POTEETE

CISSP, CGEIT, CISM, CEHv5, CRISC, VCPv5, MCSEv2k, CCAv1.x, CNEv5, ACE

1

WELCOME

- INFORMED CONSENT
- NON-DISCLOSURE AGREEMENT
- ANONYMOUS - PSEUDONYMS WILL BE USED

2

PURPOSE OF FOCUS GROUP

THIS RESEARCH IS ATTEMPTING TO DETERMINE WHICH INDIVIDUAL PREFERENCES OR SKILLS MAKE A PERSON SUCCESSFUL IN THEIR PARTICULAR CYBERSECURITY POSITION.

3

QUESTIONS - CYBERSECURITY FUNCTIONS

Do you believe that the following cybersecurity functions represent tasks performed by cybersecurity staff? (These are not job titles, but tasks performed within a role.)

Do you see any changes that would be beneficial?

- Alert Monitoring
- Creativity and Planning
- Cryptographic Implementation
- Data Forensics
- Disaster Recovery and Business Continuity
- Documentation and Cataloging
- Hardware Analysis
- Internal Reporting
- Intrusion Analysis
- Legal and Compliance Investigation
- Malware Software Analysis
- Management and Coordination
- Mission Planning
- Physical Infiltration
- Public Communication
- Public Information Dissemination
- Security Training Delivery
- Security Training Design
- Service and Product Development
- Social Engineering and Infiltration
- Technical Exploration and Penetration Testing
- Physical Implementation
- Vulnerability Communication and Disclosure

4

QUESTIONS - INTEREST CATEGORIES

Do you believe that the following interest categories would sufficiently represent various factors important to individual satisfaction or performance?

Do you see any changes that would be beneficial?

- Manual or Physical Labor
- Research and Investigation
- Creativeness and Innovation
- Sociable and Diplomatic
- Leadership and Vision
- Tolerance for Monotony

5

QUESTIONS

Organization Performance or Individual Satisfaction

Does an individual's desire to complete a task play a factor in organization performance or individual satisfaction?

Advantageous for an Organization

Would it be advantageous for an organization if they could easily align individual interests and preferences with cybersecurity job roles?

6

THANK YOU!

QUESTIONS/COMMENTS

PAUL W. POTEETE | PPOTEETE@GMAIL.COM

HTTPS://WWW.LINKEDIN.COM/IN/PAULWPOTEETE

7

C.2 Focus Group Slides

Slide	Content
Slide 1	**Research Topic: Designing an Interest-to-Function Career Alignment Model for Cybersecurity Professionals** Paul W. Poteete CISSP, CGEIT, CISM, CEHv5, CRISC, VCPv5, MCSEv2k, CCAv1.8, CNEv5, ACE
Slide 2	**Welcome** Informed Consent Non-Disclosure Agreement Anonymous - Pseudonyms will be used
Slide 3	**Purpose of Focus Group** This research is attempting to determine which individual preferences or skills make a person successful in their particular cybersecurity position.
Slide 4	**Cybersecurity Functions** Do you believe that the following cybersecurity functions represent tasks performed by cybersecurity staff? (These are not job titles, but tasks performed within a role.) Do you see any changes that would be beneficial?
Slide 5	**Interest Categories** Do you believe that the following interest categories would sufficiently represent various factors important to individual satisfaction or performance? Do you see any changes that would be beneficial?
Slide 6	**Organization Performance or Individual Satisfaction** Does an individual's desire to complete a task play a factor in organization performance or individual satisfaction? Advantageous for an Organization Would it be advantageous for an organization if they could easily align individual interests and preferences with cybersecurity job roles?
Slide 7	**Thank you!** Questions/Comments Paul W. Poteete ppoteete@gmail.com https://www.linkedin.com/in/PaulWPoteete

C.3 Participant Welcome Video

Hi, first I'd like to thank you so much for the privilege of this interview. Hopefully this research will result in improved satisfaction and performance for cybersecurity professionals and organizations around the world.

Next, I'd like to allude to the informed consent and non-disclosure agreements that are included at the beginning of this interview. Those forms simply state that all of this information will be kept anonymously, and if any information is accidentally shared or inadvertently shared with you during the interview that is identifiable to another organization you will not share that identifiable information. During the interview it's very unlikely this would happen but just to be sure we need to keep everything confidential.

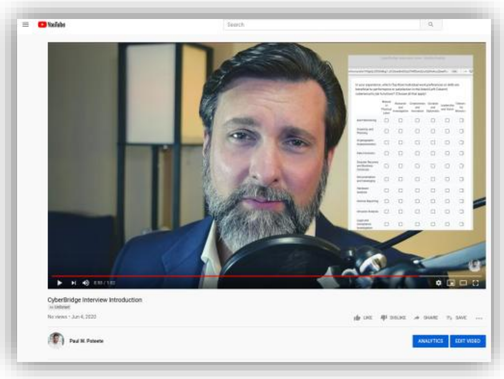
Finally, I'd like to go over the interview questions with you directly. At the beginning of the interview you'll see the informed consent and the non-disclosure agreement. After reading those and understanding the survey is anonymous and it is an interview then choose next as you go into the interview.

Which country do you currently reside? You can pick any of those countries or you can choose not to answer. Which category do you consider your position to reside, and that would be do you consider yourself as staff or management, and how many years of cybersecurity experience do you have in your position? (That could be throughout your entire lifetime).

Now, individual preferences, when we're discussing individual preferences, we're discussing policy creation and administration. What deployment investigation and creativity, what individual preference would be beneficial to this actual function? So over on the left hand side you'll see all of our functions. About 30 functions are listed. Then we can say this person would be mostly interested in deploying systems, or investigative kind of preference, or they have a creative preference, or they really like socializing? Would that work with policy creation and administration? What kind of things would be in there or management and coordination? Would a person who does management coordination be interested in deployment? (which would be kind of hands-on). Or would they be mainly leaning towards a leadership orientation or a socializing type orientation? Would that be creative investigatory? Would they be an investigator or something like that? Would those traits be best suited for that individual?

After you do individual preferences, next would be the functions, if you could define those functions. For instance, operational functions. We have operational, defensive, and offensive functions. So if you're looking at operational functions policy creation administration, does that fit in the current category or should we move that to defensive or offensive? Or is that a duplicate of something else and we should delete it? If you do see a duplicate just choose to delete one of them. If you want, you could choose both. I'll be reading it so I'll figure it out. On the defensive functions, if you'll go through defensive functions and the same thing there is defensive play and design, should we move that operational? Should we move the offensive? Then we go to offensive playing design. Should we keep it in the category? Some of those actually have the words in there that are used.

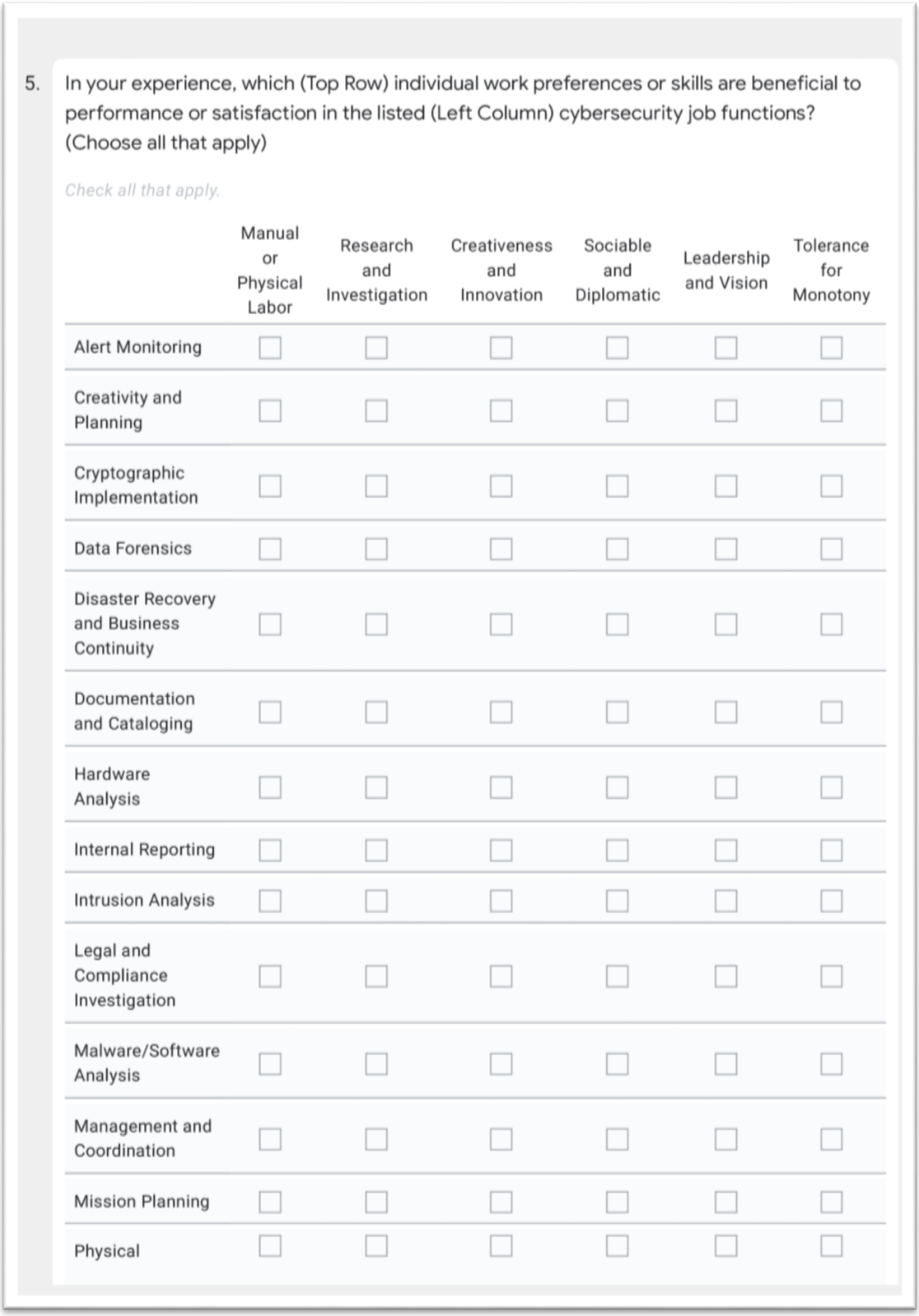
Finally, there are sections for comments throughout the interview. I encourage you to share comments about the interview and what could be changed about the actual research itself. If you do find anything that needs to be changed, I appreciate your input. This is your opinion based on your professional your personal experience. It is simply your input whatever you say is valid. I thank you again for the opportunity for this interview.



C.4 Expert Interview Questions - Part 1

Expert Interview Questions – Part 1
The purpose of this individual interview is to collect data about cybersecurity roles and career preferences that may assist in the overall improvement of the results of this research. The interview results are anonymous; however, I must collect your email address for ethics verification. Again, neither your name or email will be listed in the final document or any associated research. * Required 1. Email address * CyberBridge Interview Introduction (Video)
2. Do you agree with the Anonymous nature of the Informed Consent and Non-Disclosure of any information that may be somehow shared during this survey? Required Documents: http://www.CyberBridge.me/docs/NDA.pdf http://www.CyberBridge.me/docs/InformedConsent.pdf * Yes No
3. What do you consider your position to be? * Staff Management
4. How many cybersecurity-related years of experience do you possess? * 0-1 year 1-5 years 5-10 years 10 or more years
5. In your experience, which (Top Row) individual work preferences or skills are beneficial to performance or satisfaction in the listed (Left Column) cybersecurity job functions? (Choose all that apply) Column Headings: Manual or Physical Labor Research and Investigation Creativeness and Innovation Sociable and Diplomatic Leadership and Vision Tolerance for Monotony Row Headings: Alert Monitoring Creativity and Planning Cryptographic Implementation Data Forensics Disaster Recovery and Business Continuity Documentation and Cataloging

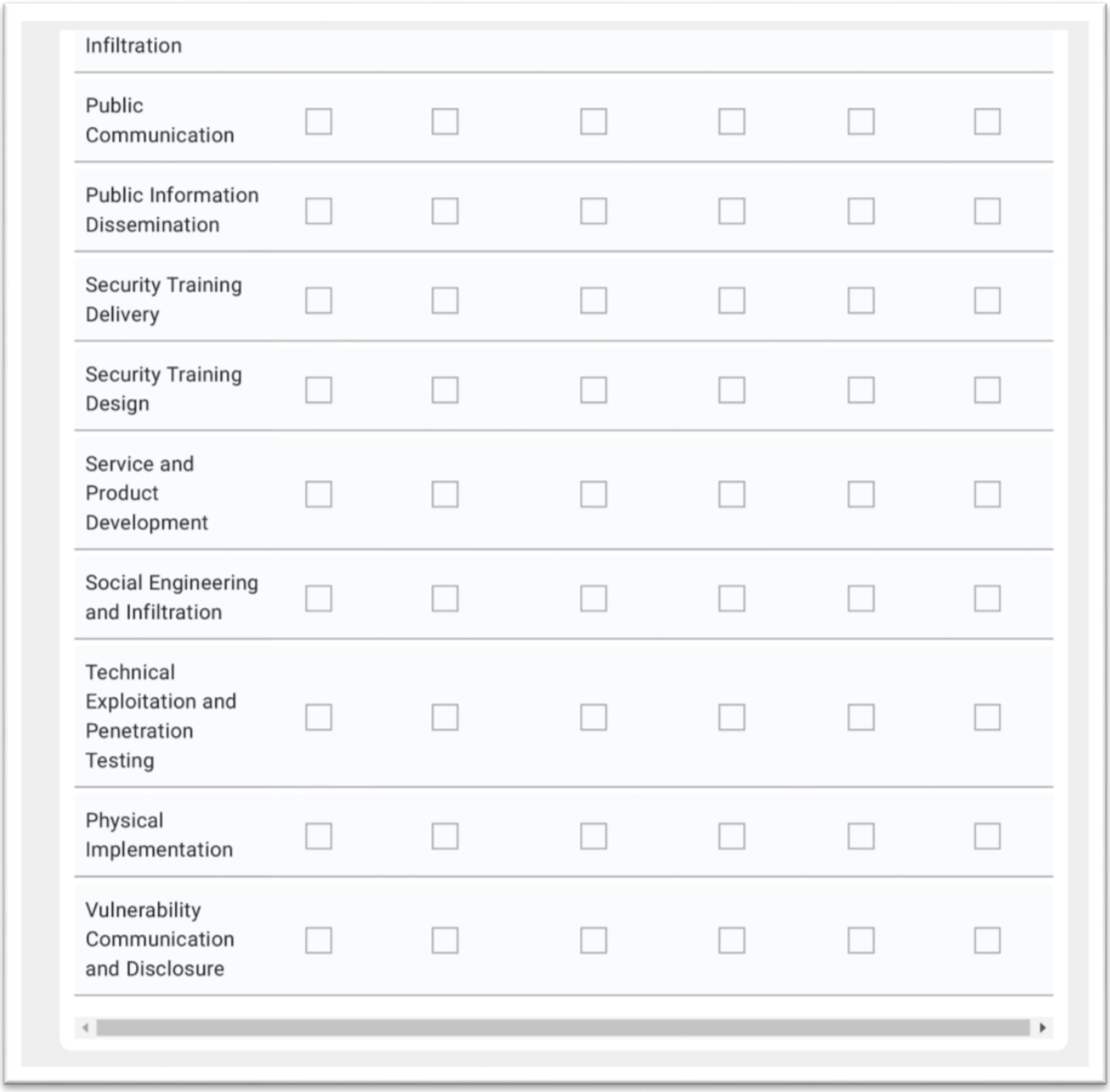
Hardware Analysis
Internal Reporting
Intrusion Analysis
Legal and Compliance Investigation
Malware/Software Analysis
Management and Coordination
Mission Planning
Physical Infiltration
Public Communication
Public Information Dissemination
Security Training Delivery
Security Training Design
Service and Product Development
Social Engineering and Infiltration
Technical Exploitation and Penetration Testing
Physical Implementation
Vulnerability Communication and Disclosure



5. In your experience, which (Top Row) individual work preferences or skills are beneficial to performance or satisfaction in the listed (Left Column) cybersecurity job functions? (Choose all that apply)

Check all that apply.

	Manual or Physical Labor	Research and Investigation	Creativeness and Innovation	Sociable and Diplomatic	Leadership and Vision	Tolerance for Monotony
Alert Monitoring	□	□	□	□	□	□
Creativity and Planning	□	□	□	□	□	□
Cryptographic Implementation	□	□	□	□	□	□
Data Forensics	□	□	□	□	□	□
Disaster Recovery and Business Continuity	□	□	□	□	□	□
Documentation and Cataloging	□	□	□	□	□	□
Hardware Analysis	□	□	□	□	□	□
Internal Reporting	□	□	□	□	□	□
Intrusion Analysis	□	□	□	□	□	□
Legal and Compliance Investigation	□	□	□	□	□	□
Malware/Software Analysis	□	□	□	□	□	□
Management and Coordination	□	□	□	□	□	□
Mission Planning	□	□	□	□	□	□
Physical	□	□	□	□	□	□



Infiltration						
Public Communication	□	□	□	□	□	□
Public Information Dissemination	□	□	□	□	□	□
Security Training Delivery	□	□	□	□	□	□
Security Training Design	□	□	□	□	□	□
Service and Product Development	□	□	□	□	□	□
Social Engineering and Infiltration	□	□	□	□	□	□
Technical Exploitation and Penetration Testing	□	□	□	□	□	□
Physical Implementation	□	□	□	□	□	□
Vulnerability Communication and Disclosure	□	□	□	□	□	□

6. Your input is very important. Please list any additional opinions or comments about the interview, cybersecurity functions, or individual traits here. Thank you for your time and experience!

C.4 Expert Interview Questions - Part 2

Expert Interview Questions - Part 2

Please comment on the 1) Individual Preferences and 2) Cybersecurity Functions below.

What does this mean?

In the chart listed below, please select Remove or Confusing, if you feel that the "Individual Preference" does not relate to any cybersecurity-related task, or if the "Cybersecurity Function" does not relate to Cybersecurity, as a whole.

Please add any Preferences or Functions in the comment field below each option.

1. Your email address will NOT be revealed. It is only require for 1) to receive your copy of the responses and 2) for the Research Ethics Committee to verify that I have not committed any ethical violations in the case of any concern. Again, your personal information or email address will NOT be associated with your answers in the research data report.

Email address *

2. Do you agree with the Anonymous nature of the Informed Consent and Non-Disclosure of any information that may be somehow shared during this survey? *

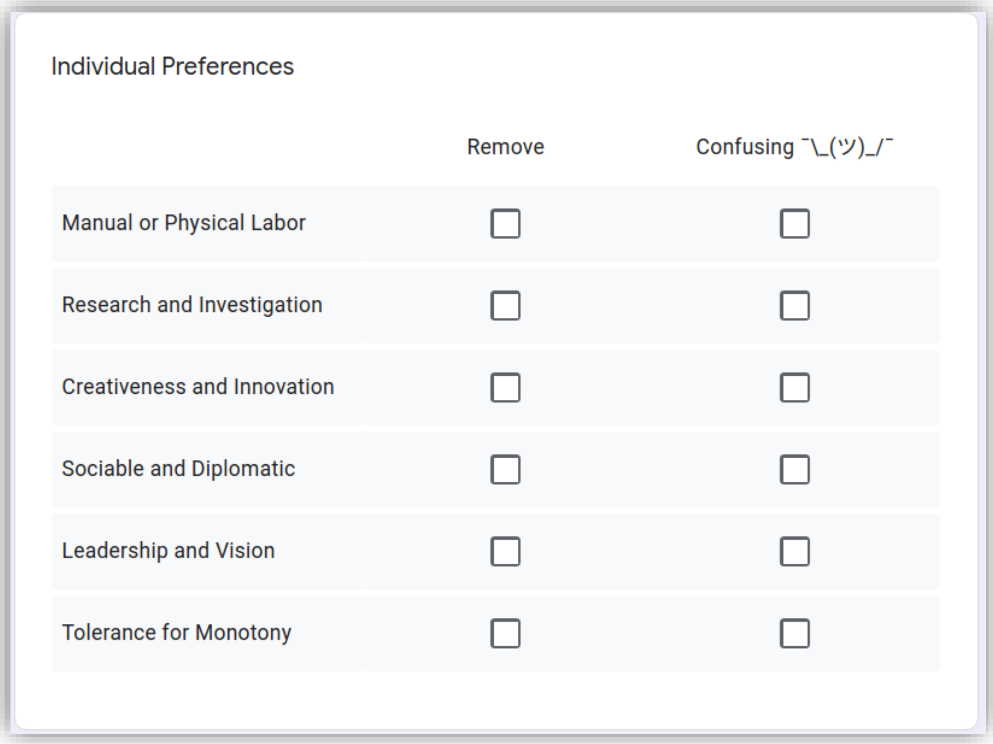
Yes

No

3. Individual Preferences

Column Headings:
Remove
Confusing ¯_(ツ)_/¯

Row Headings:
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony



Individual Preferences

	Remove	Confusing ¯_(ツ)_/¯
Manual or Physical Labor	□	□
Research and Investigation	□	□
Creativeness and Innovation	□	□
Sociable and Diplomatic	□	□
Leadership and Vision	□	□
Tolerance for Monotony	□	□

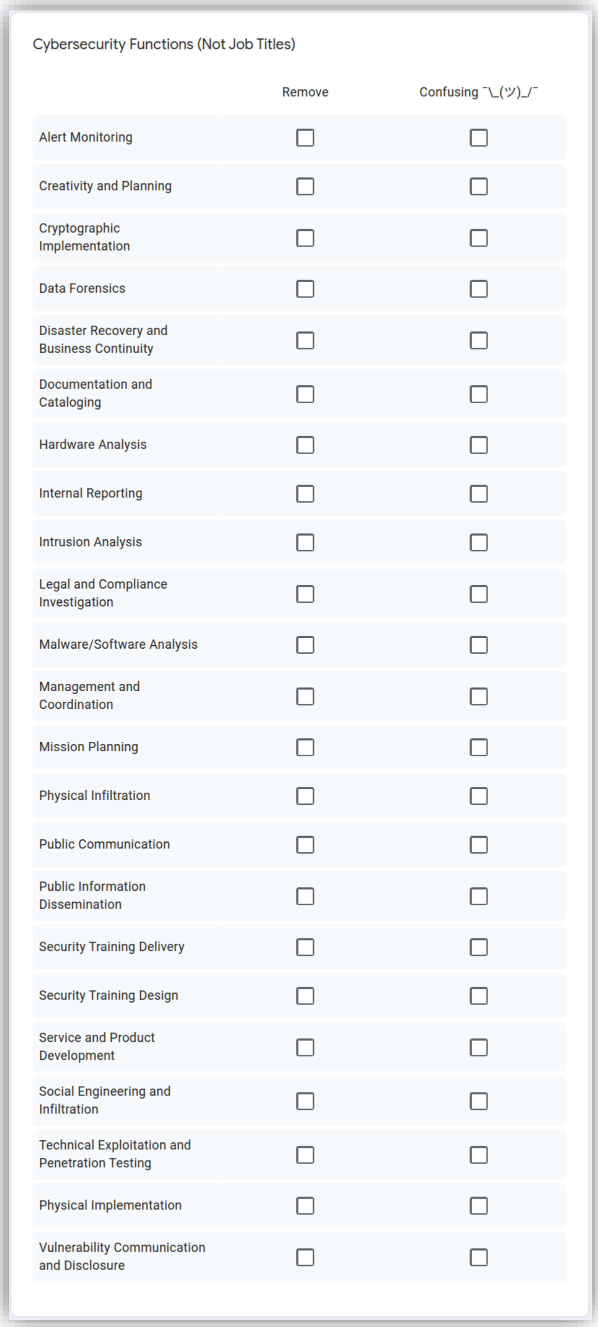
4. Individual Work Preferences or Affinity: Are there any personal preferences that are missing from the above list? Is there anything that you would like to change?

5. Cybersecurity Functions (Not Job Titles)

Column Headings:
Remove
Confusing ¯_(ツ)_/¯

Row Headings:
Alert Monitoring
Creativity and Planning
Cryptographic Implementation
Data Forensics
Disaster Recovery and Business Continuity
Documentation and Cataloging
Hardware Analysis
Internal Reporting
Intrusion Analysis
Legal and Compliance Investigation
Malware/Software Analysis
Management and Coordination
Mission Planning
Physical Infiltration

Public Communication
Public Information Dissemination
Security Training Delivery
Security Training Design
Service and Product Development
Social Engineering and Infiltration
Technical Exploitation and
Penetration Testing
Physical Implementation
Vulnerability Communication and Disclosure



Cybersecurity Functions (Not Job Titles)

	Remove	Confusing ¯_(ツ)_/¯
Alert Monitoring	□	□
Creativity and Planning	□	□
Cryptographic Implementation	□	□
Data Forensics	□	□
Disaster Recovery and Business Continuity	□	□
Documentation and Cataloging	□	□
Hardware Analysis	□	□
Internal Reporting	□	□
Intrusion Analysis	□	□
Legal and Compliance Investigation	□	□
Malware/Software Analysis	□	□
Management and Coordination	□	□
Mission Planning	□	□
Physical Infiltration	□	□
Public Communication	□	□
Public Information Dissemination	□	□
Security Training Delivery	□	□
Security Training Design	□	□
Service and Product Development	□	□
Social Engineering and Infiltration	□	□
Technical Exploitation and Penetration Testing	□	□
Physical Implementation	□	□
Vulnerability Communication and Disclosure	□	□

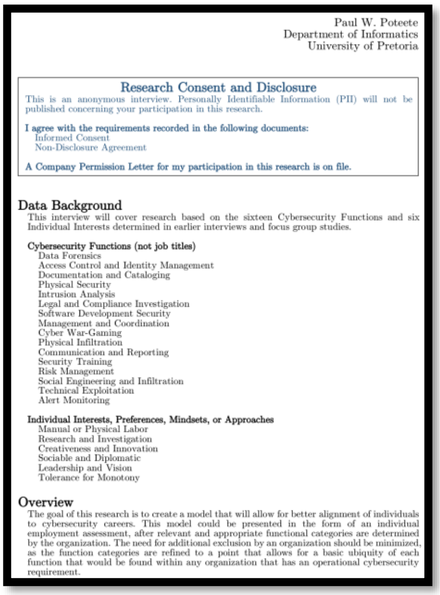
6. Cybersecurity Functions: Are there any functions missing from the above list? Is there anything that you would like to change?
7. Would you like to be contacted for an ADDITIONAL Group Forum (Online or In-Person), Individual Interview (Online or In-Person), or Survey for this research? (Note: This research should conclude in about 1 month. It will be released internationally for business management and cybersecurity influence sectors) Yes No

C.5 Confirmatory Interview Questions

Personal Research Interview
Paul W. Poteete
Department of Informatics
University of Pretoria

Research Consent and Disclosure

This is an anonymous interview. Personally Identifiable Information (PII) will not be
published concerning your participation in this research.
I agree with the requirements recorded in the following documents:
Informed Consent
Non-Disclosure Agreement
A Company Permission Letter for my participation in this research is on file.



Paul W. Poteete
Department of Informatics
University of Pretoria

Research Consent and Disclosure

This is an anonymous interview. Personally Identifiable Information (PII) will not be published concerning your participation in this research.

I agree with the requirements recorded in the following documents:
Informed Consent
Non-Disclosure Agreement

A Company Permission Letter for my participation in this research is on file.

Data Background

This interview will cover research based on the sixteen Cybersecurity Functions and six Individual Interests determined in earlier interviews and focus group studies.

Cybersecurity Functions (not job titles)
Data Forensics
Access Control and Identity Management
Documentation and Cataloging
Physical Security
Intrusion Analysis
Legal and Compliance Investigation
Software Development Security
Management and Coordination
Cyber War-Gaming
Physical Infiltration
Communication and Reporting
Security Training
Risk Management
Social Engineering and Infiltration
Technical Exploitation
Alert Monitoring

Individual Interests, Preferences, Mindsets, or Approaches
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony

Overview

The goal of this research is to create a model that will allow for better alignment of individuals to cybersecurity careers. This model could be presented in the form of an individual employment assessment, after relevant and appropriate functional categories are determined by the organization. The need for additional exclusion by an organization should be minimized, as the function categories are refined to a point that allows for a basic ubiquity of each function that would be found within any organization that has an operational cybersecurity requirement.

Data Background

This interview will cover research based on the sixteen Cybersecurity Functions and six

Individual Interests determined in earlier interviews and focus group studies.

Cybersecurity Functions (not job titles)

- Data Forensics
- Access Control and Identity Management
- Documentation and Cataloging
- Physical Security
- Intrusion Analysis
- Legal and Compliance Investigation
- Software Development Security
- Management and Coordination
- Cyber War-Gaming
- Physical Infiltration
- Communication and Reporting
- Security Training
- Risk Management
- Social Engineering and Infiltration
- Technical Exploitation
- Alert Monitoring
- Individual Interests, Preferences, Mindsets, or Approaches
- Manual or Physical Labor
- Research and Investigation
- Creativeness and Innovation
- Sociable and Diplomatic
- Leadership and Vision
- Tolerance for Monotony

Overview

The goal of this research is to create a model that will allow for better alignment of individuals to cybersecurity careers. This model could be presented in the form of an individual employment assessment, after relevant and appropriate functional categories are determined by the organization. The need for additional exclusion by an organization should be minimized, as the function categories are refined to a point that allows for a basic ubiquity of each function that would be found within any organization that has an operational cybersecurity requirement.

Confirmatory Interview Questions

Section 1: Demographics

These data points allow for some differentiation in individual opinion and data visualization. They are not known to be of direct value to the current research directives; however, they may prove to clarify some points in the final evaluation phase.

1. In which country do you currently reside?
2. How many years of experience do you possess with cybersecurity functions?
3. Are you representing a Management or Staff function within this interview?

Section 2: Program Viability

Based on the scope of this specific research, there may be several factors that should be included in future research. In some cases, these factors could augment the current research. In order to properly determine the direction of these comments, please discuss your personal impression of the research goals.

4. Do you feel that aligning and employee's "Individual Interests" with "Cybersecurity Functions" could be advantageous for a firm and the individual? yes/no. Please explain.

Section 3: Challenges and Rewards

In order for the model to properly evaluate individual interests and functions, both respective parties must understand their own needs and motivations.

5. What are the potential rewards for an organization that aligns Individual Interests to Organizational Cybersecurity Functions? (for the individual, organization, industry, society)

6. What are the potential difficulties in defining the following concepts to an individual and organization?

Cybersecurity Functions
Individual Interests
Interest-to-Function Alignment

C.6 Job Functions Survey Questions

Job Functions Survey Questions

The goal is to create the most condensed data set while maintaining an accurate representation of the data. NOTE: These are not cybersecurity job titles, but simply cybersecurity job functions

* Required

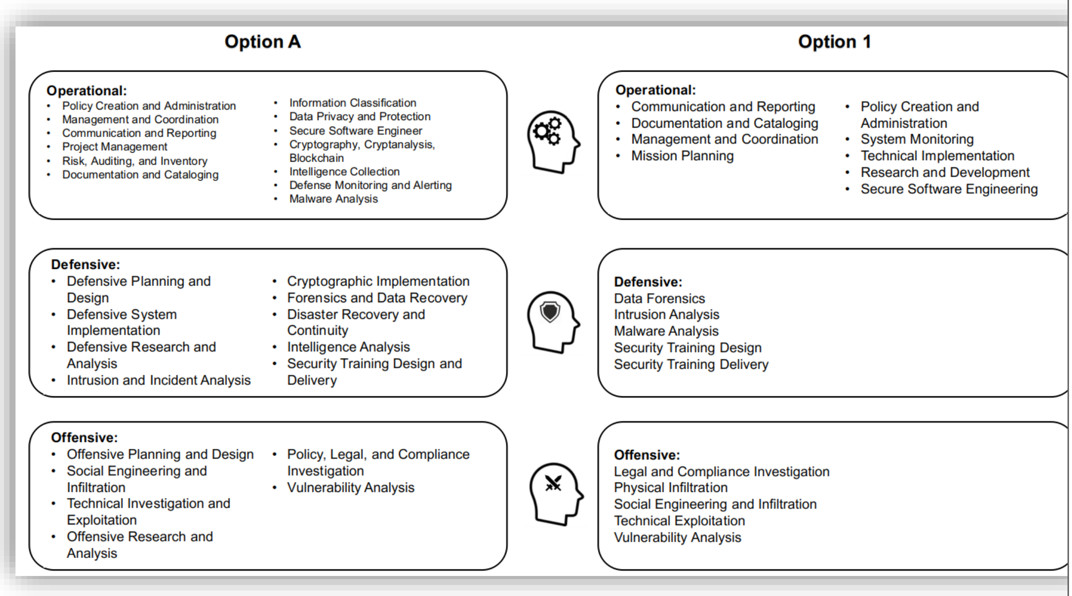
1. Do you agree with the Anonymous nature of the Informed Consent and Non-Disclosure of any information that may be somehow shared during this survey?

Mark only one oval.

Yes

No

2. Which of the two categorizations do you feel is most closely achieves this goal? Option A or Option 1



Option A

Operational:
- Policy Creation and Administration
- Management and Coordination
- Communication and Reporting
- Project Management
- Risk, Auditing, and Inventory
- Documentation and Cataloging
- Information Classification
- Data Privacy and Protection
- Secure Software Engineer
- Cryptography, Cryptanalysis, Blockchain
- Intelligence Collection
- Defense Monitoring and Alerting
- Malware Analysis

Defensive:
- Defensive Planning and Design
- Defensive System Implementation
- Defensive Research and Analysis
- Intrusion and Incident Analysis
- Cryptographic Implementation
- Forensics and Data Recovery
- Disaster Recovery and Continuity
- Intelligence Analysis
- Security Training Design and Delivery

Offensive:
- Offensive Planning and Design
- Social Engineering and Infiltration
- Technical Investigation and Exploitation
- Offensive Research and Analysis
- Policy, Legal, and Compliance Investigation
- Vulnerability Analysis

Option 1

Operational:
- Communication and Reporting
- Documentation and Cataloging
- Management and Coordination
- Mission Planning
- Policy Creation and Administration
- System Monitoring
- Technical Implementation
- Research and Development
- Secure Software Engineering

Defensive:

Data Forensics
Intrusion Analysis
Malware Analysis
Security Training Design
Security Training Delivery

Offensive:

Legal and Compliance Investigation
Physical Infiltration
Social Engineering and Infiltration
Technical Exploitation
Vulnerability Analysis

Mark only one oval.

Option A

Option 1

3. Under the option that you selected, if there are any functions that are too specific or duplicates that should be removed, please let me know what those might be.

C.7. Focus Group Questions

Forum Title: Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions

Collect data from cybersecurity professionals concerning cybersecurity roles and career preferences for this research.

Cybersecurity Functions

Do you believe that the following cybersecurity functions represent tasks performed by cybersecurity staff?

(These are not job titles, but tasks performed within a role.)

Do you see any changes that would be beneficial?

Alert Monitoring
Creativity and Planning
Cryptographic Implementation
Data Forensics
Disaster Recovery and Business Continuity
Documentation and Cataloging
Hardware Analysis
Internal Reporting
Intrusion Analysis
Legal and Compliance Investigation
Malware/Software Analysis
Management and Coordination
Mission Planning
Physical Infiltration
Public Communication
Public Information Dissemination
Security Training Delivery
Security Training Design
Service and Product Development
Social Engineering and Infiltration
Technical Exploitation and Penetration Testing
Physical Implementation
Vulnerability Communication and Disclosure

Interest Categories

Do you believe that the following interest categories would sufficiently represent various factors important to individual satisfaction or performance?

Do you see any changes that would be beneficial?

Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony

Organization Performance or Individual Satisfaction

Does an individual's desire to complete a task play a factor in organization performance or individual satisfaction?

Advantageous for an Organization

Would it be advantageous for an organization if they could easily align individual interests and preferences with cybersecurity job roles?

C.8. Cybersecurity Interest-to-Function Survey Questions

Cybersecurity Interest-to-Function Survey

This is an anonymous survey for cybersecurity professionals. No personally identifiable information is requested or retained.

The goal of this survey is to improve employee satisfaction and organizational performance by designing an effective system to align cybersecurity work preferences or skills to specific cybersecurity job functions.

Your input is greatly appreciated!

* Required

1.My primary job function(s) pertains to cybersecurity as listed in at least one of the cybersecurity job functions below. *

Mark only one oval.

Yes - My job function(s) pertain to cybersecurity as listed in at least one of the cybersecurity job functions listed.

No - My job functions do not relate to cybersecurity. If no, your experience is outside the scope of this research study. Thank you for your time.

Informed Consent
2. I agree with the anonymous nature of the Informed Consent. *
Mark only one oval.
Yes
No

Basic Demographics
3. What is your current job title?

4. What do you consider your position to be? *
Mark only one oval.
Staff
Management

5. How many cybersecurity-related years of experience do you possess? *
Mark only one oval.
0-1 year
1-5 years
5-10 years
10 or more years

6. In which country do you currently reside? *
Mark only one oval.

Data Forensics
7. Have you had experience with Data Forensics? *
Mark only one oval.
Yes - Skip to question 8
No - Skip to question 9

Data Forensics - Individual Skills and Abilities
8. In your experience, which individual trait, mindset, or approach is most beneficial when working with data forensics?
Mark only one oval.
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony

Access Control and Identity Management
9. Have you had experience with Access Control or Identity Management? *
Mark only one oval.
Yes - Skip to question 10
No - Skip to question 11

Access Control and Identity Management - Individual Skills and Abilities
10. In your experience, which individual trait, mindset, or approach is most beneficial when creating access and identity management controls?
Mark only one oval.
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony

Documentation and Cataloging
11. Have you had experience providing Documentation and Cataloging? *
Mark only one oval.
Yes - Skip to question 12
No - Skip to question 13

Documentation and Cataloging - Individual Skills and Abilities
12. In your experience, which individual trait, mindset, or approach is most beneficial when documenting and cataloging?
Mark only one oval.
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision

Tolerance for Monotony

Physical Security
13. Have you had experience with Physical Security? *
Mark only one oval.
Yes - Skip to question 14
No - Skip to question 15

Physical Security - Individual Skills and Abilities
14. In your experience, which individual trait, mindset, or approach is most beneficial when working with the physical security of an organization?
Mark only one oval.
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony

Intrusion Analysis
15. Have you had experience with Intrusion Analysis? *
Mark only one oval.
Yes - Skip to question 16
No - Skip to question 17

Intrusion Analysis - Individual Skills and Abilities
16. In your experience, which individual trait, mindset, or approach is most beneficial when analyzing intrusions?
Mark only one oval.
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony

Legal and Compliance Investigation
17. Have you had experience with Legal and Compliance Investigations? *
Mark only one oval.
Yes - Skip to question 18
No - Skip to question 19

Legal and Compliance Investigation - Individual Skills and Abilities
18. In your experience, which individual trait, mindset, or approach is most beneficial when investigating legal and compliance data for an organization?
Mark only one oval.
Manual or Physical Labor

Research and Investigation Creativeness and Innovation Sociable and Diplomatic Leadership and Vision Tolerance for Monotony
Software Development Security 19. Have you had experience with Software Development Security? * Mark only one oval. Yes - Skip to question 20 No - Skip to question 21
Software Development Security - Individual Skills and Abilities 20. In your experience, which individual trait, mindset, or approach is most beneficial when developing software securely? Mark only one oval. Manual or Physical Labor Research and Investigation Creativeness and Innovation Sociable and Diplomatic Leadership and Vision Tolerance for Monotony
Management and Coordination 21. Have you had experience with Management and Coordination? * Mark only one oval. Yes - Skip to question 22 No - Skip to question 23
Management and Coordination - Individual Skills and Abilities 22. In your experience, which individual trait, mindset, or approach is most beneficial when managing or coordinating teams at an organization? Mark only one oval. Manual or Physical Labor Research and Investigation Creativeness and Innovation Sociable and Diplomatic Leadership and Vision Tolerance for Monotony
Cyber Wargaming 23. Have you had experience with Cyber Wargaming? * Mark only one oval. Yes - Skip to question 24 No - Skip to question 25
Cyber Wargaming - Individual Skills and Abilities

24. In your experience, which individual trait, mindset, or approach is most beneficial when you conducting cyber wargaming?

Mark only one oval.

Manual or Physical Labor

Research and Investigation

Creativeness and Innovation

Sociable and Diplomatic

Leadership and Vision

Tolerance for Monotony

Physical Infiltration

25. Have you had experience with Physical Infiltration? *

Mark only one oval.

Yes - Skip to question 26

No - Skip to question 27

Physical Infiltration - Individual Skills and Abilities

26. In your experience, which individual trait, mindset, or approach is most beneficial when physically infiltrating a target site?

Mark only one oval.

Manual or Physical Labor

Research and Investigation

Creativeness and Innovation

Sociable and Diplomatic

Leadership and Vision

Tolerance for Monotony

Communication and Reporting

27. Have you had experience with Communication and Reporting? *

Mark only one oval.

Yes - Skip to question 28

No - Skip to question 29

Communication and Reporting - Individual Skills and Abilities

28. In your experience, which individual trait, mindset, or approach is most beneficial when communicating and reporting data within an organization?

Mark only one oval.

Manual or Physical Labor

Research and Investigation

Creativeness and Innovation

Sociable and Diplomatic

Leadership and Vision

Tolerance for Monotony

Security Training

29. Have you had experience with instructing Security Training? *

Mark only one oval.

Yes - Skip to question 30

No - Skip to question 31

Security Training - Individual Skills and Abilities

30. In your experience, which individual trait, mindset, or approach is most beneficial when conducting security training?

Mark only one oval.
Manual or Physical Labor

Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony

Risk Management

31. Have you had experience with Risk Management? *

Mark only one oval.
Yes - Skip to question 32
No - Skip to question 33

Risk Management - Individual Skills and Abilities

32. In your experience, which individual trait, mindset, or approach is most beneficial when performing risk management functions?

Mark only one oval.
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony

Social Engineering and Infiltration

33. Have you had experience with Social Engineering and Infiltration? *

Mark only one oval.
Yes - Skip to question 34
No - Skip to question 35

Social Engineering and Infiltration - Individual Skills and Abilities

34. In your experience, which individual trait, mindset, or approach is most beneficial when conducting social engineering and infiltration?

Mark only one oval.
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony

Technical Exploitation

35. Have you had experience with Technical Exploitation? *

Mark only one oval.

Yes - Skip to question 36

No - Skip to question 37

Technical Exploitation - Individual Skills and Abilities

36. In your experience, which individual trait, mindset, or approach is most beneficial when penetration testing or exploitation?

Mark only one oval.

Manual or Physical Labor

Research and Investigation

Creativeness and Innovation

Sociable and Diplomatic

Leadership and Vision

Tolerance for Monotony

Alert Monitoring

37. Have you had experience with Alert Monitoring? *

Mark only one oval.

Yes - Skip to question 38

No - Skip to question 39

Alert Monitoring - Individual Skills and Abilities and Abilities

38. In your experience, which individual trait, mindset, or approach is most beneficial when monitoring the alerts for an organization?

Mark only one oval.

Manual or Physical Labor

Research and Investigation

Creativeness and Innovation

Sociable and Diplomatic

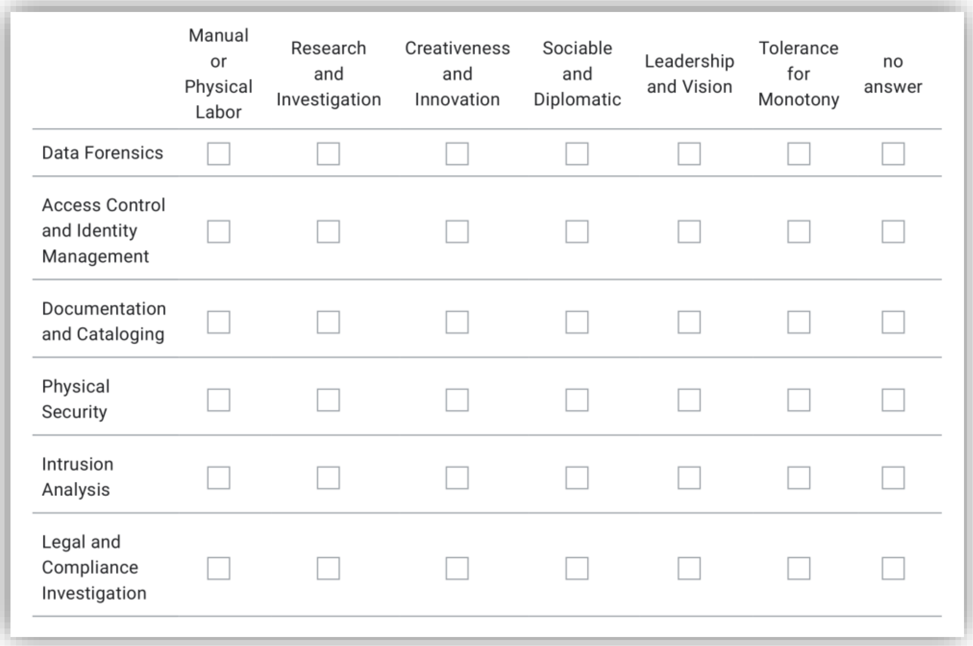
Leadership and Vision

Tolerance for Monotony

Complete Job Functions Chart

39. PART 1:3 - In your experience, choose up to 3 boxes (Top Row) for individual work preferences or skills are MOST beneficial to performance or satisfaction for the listed (Left Column) cybersecurity job functions?

Check all that apply.



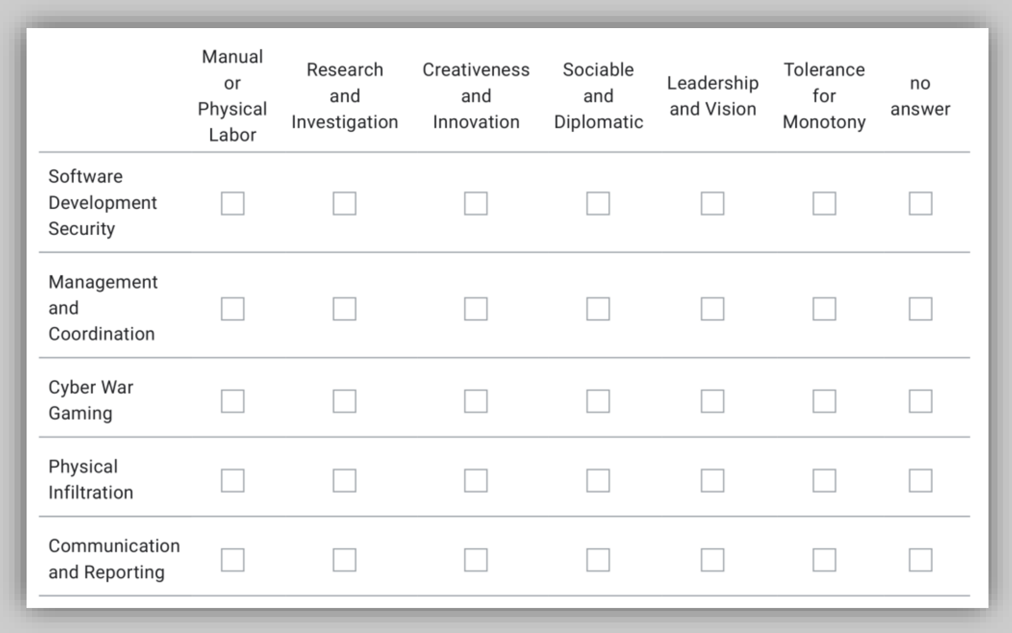
	Manual or Physical Labor	Research and Investigation	Creativeness and Innovation	Sociable and Diplomatic	Leadership and Vision	Tolerance for Monotony	no answer
Data Forensics	□	□	□	□	□	□	□
Access Control and Identity Management	□	□	□	□	□	□	□
Documentation and Cataloging	□	□	□	□	□	□	□
Physical Security	□	□	□	□	□	□	□
Intrusion Analysis	□	□	□	□	□	□	□
Legal and Compliance Investigation	□	□	□	□	□	□	□

Column Headings:
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony
no answer

Row Headings:
Data Forensics
Access Control and Identity Management
Documentation and Cataloging
Physical Security
Intrusion Analysis
Legal and Compliance Investigation
Data Forensics
Access Control and Identity Management
Documentation and Cataloging
Physical Security
Intrusion Analysis
Legal and Compliance Investigation

40. PART 2:3 - In your experience, choose up to 3 boxes (Top Row) for individual work preferences or skills are MOST beneficial to performance or satisfaction for the listed (Left Column) cybersecurity job functions?

Check all that apply.



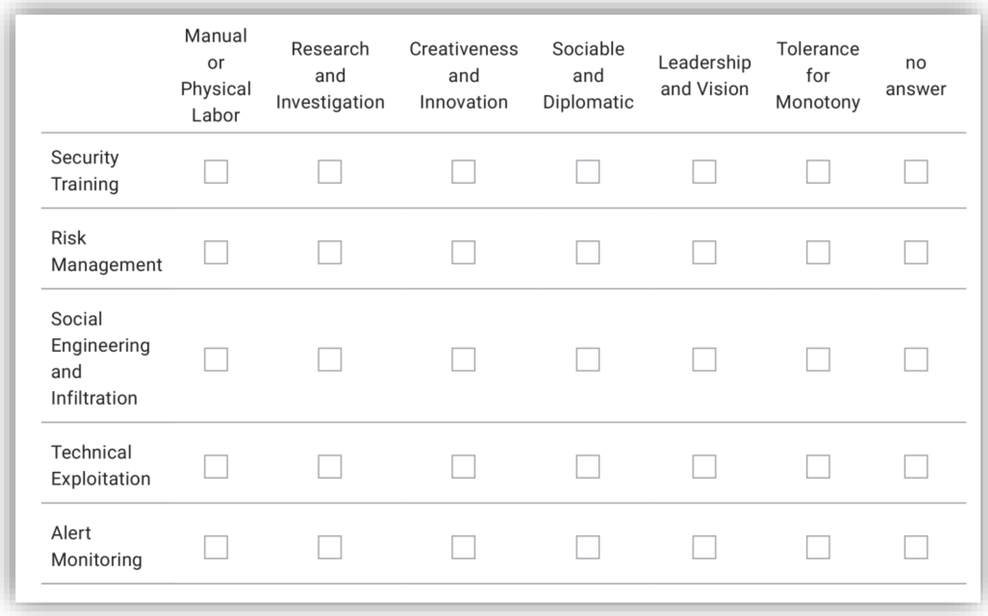
	Manual or Physical Labor	Research and Investigation	Creativeness and Innovation	Sociable and Diplomatic	Leadership and Vision	Tolerance for Monotony	no answer
Software Development Security	□	□	□	□	□	□	□
Management and Coordination	□	□	□	□	□	□	□
Cyber War Gaming	□	□	□	□	□	□	□
Physical Infiltration	□	□	□	□	□	□	□
Communication and Reporting	□	□	□	□	□	□	□

Column Headings:
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony
no answer

Row Headings:
Software Development Security
Management and Coordination
Cyber War Gaming
Physical Infiltration
Communication and Reporting
Software Development Security
Management and Coordination
Cyber War Gaming
Physical Infiltration
Communication and Reporting

41. PART 3:3 - In your experience, choose up to 3 boxes (Top Row) for individual work preferences or skills are MOST beneficial to performance or satisfaction for the listed (Left Column) cybersecurity job functions?

Check all that apply.

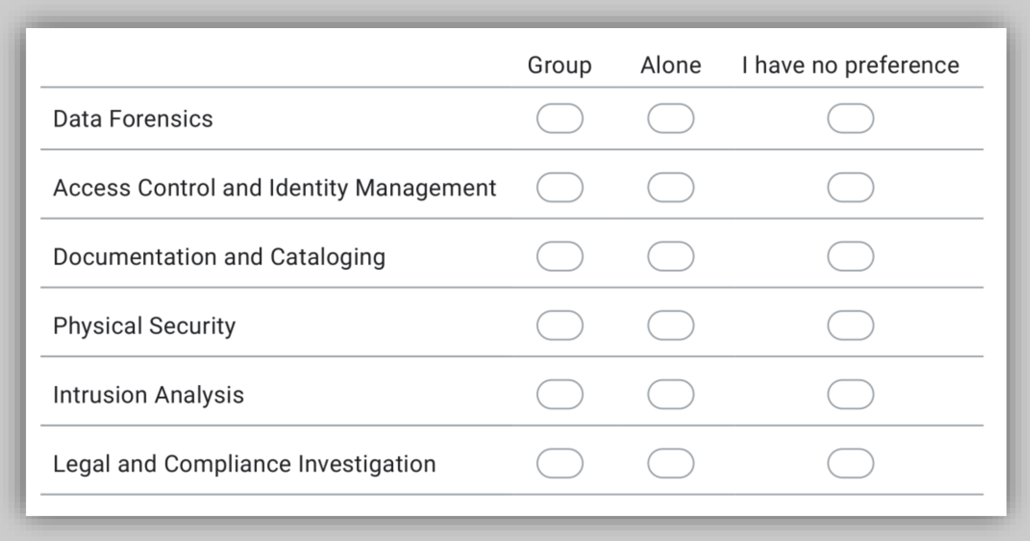


	Manual or Physical Labor	Research and Investigation	Creativeness and Innovation	Sociable and Diplomatic	Leadership and Vision	Tolerance for Monotony	no answer
Security Training	□	□	□	□	□	□	□
Risk Management	□	□	□	□	□	□	□
Social Engineering and Infiltration	□	□	□	□	□	□	□
Technical Exploitation	□	□	□	□	□	□	□
Alert Monitoring	□	□	□	□	□	□	□

Column Headings:
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony
no answer

Row Headings:
Security Training
Risk Management
Social Engineering and Infiltration
Technical Exploitation
Alert Monitoring
Security Training
Risk Management
Social Engineering and Infiltration
Technical Exploitation
Alert Monitoring

42. Part 1:3 - In your opinion, would each function be best performed while working in a group or alone? (what is your preference?)
Mark only one oval per row.

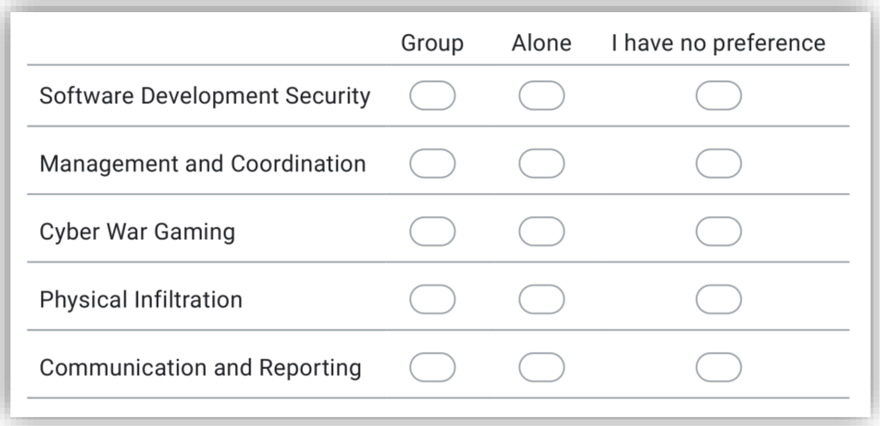


	Group	Alone	I have no preference
Data Forensics	○	○	○
Access Control and Identity Management	○	○	○
Documentation and Cataloging	○	○	○
Physical Security	○	○	○
Intrusion Analysis	○	○	○
Legal and Compliance Investigation	○	○	○

Column Headings:
Group
Alone
I have no preference

Row Headings:
Data Forensics
Access Control and Identity Management
Documentation and Cataloging
Physical Security
Intrusion Analysis
Legal and Compliance Investigation
Data Forensics
Access Control and Identity Management
Documentation and Cataloging
Physical Security
Intrusion Analysis
Legal and Compliance Investigation

43. Part 2:3 - In your opinion, would each function be best performed while working in a group or alone? (what is your preference?)
Mark only one oval per row.



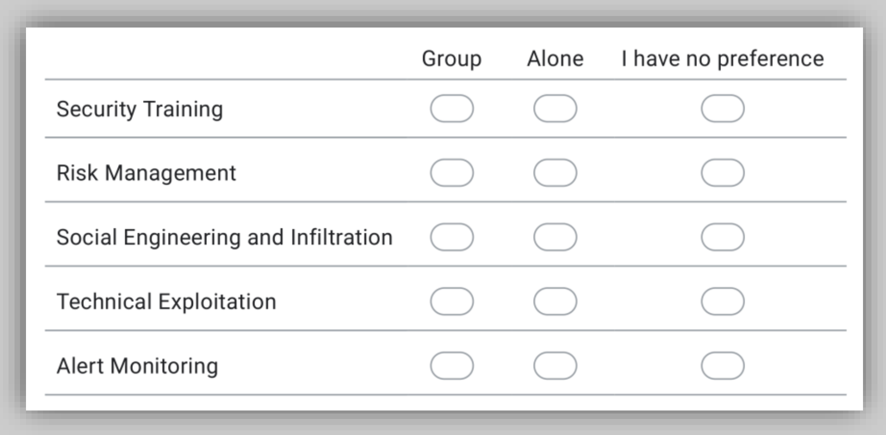
	Group	Alone	I have no preference
Software Development Security	○	○	○
Management and Coordination	○	○	○
Cyber War Gaming	○	○	○
Physical Infiltration	○	○	○
Communication and Reporting	○	○	○

Column Headings:
Group
Alone
I have no preference

Row Headings:
Software Development Security
Management and Coordination
Cyber War Gaming
Physical Infiltration
Communication and Reporting
Software Development Security
Management and Coordination
Cyber War Gaming
Physical Infiltration
Communication and Reporting

44. Part 3:3 - In your opinion, would each function be best performed while working in a
grou

p or alone? (what is your preference?)
Mark only one oval per row.



	Group	Alone	I have no preference
Security Training	○	○	○
Risk Management	○	○	○
Social Engineering and Infiltration	○	○	○
Technical Exploitation	○	○	○
Alert Monitoring	○	○	○

Column Headings:
Group

Alone
I have no preference

Row Headings:
Security Training
Risk Management
Social Engineering and Infiltration
Technical Exploitation
Alert Monitoring
Security Training
Risk Management
Social Engineering and Infiltration
Technical Exploitation
Alert Monitoring

45. Please include any information regarding the length or difficulty of the survey. Thank you again for your time and experience!

Thank you

Your opinion is greatly appreciated.

Please include any comments
or improvements to the survey below.

C.9. Final Survey Questions

Cybersecurity Interest-to-Function Survey Final Survey

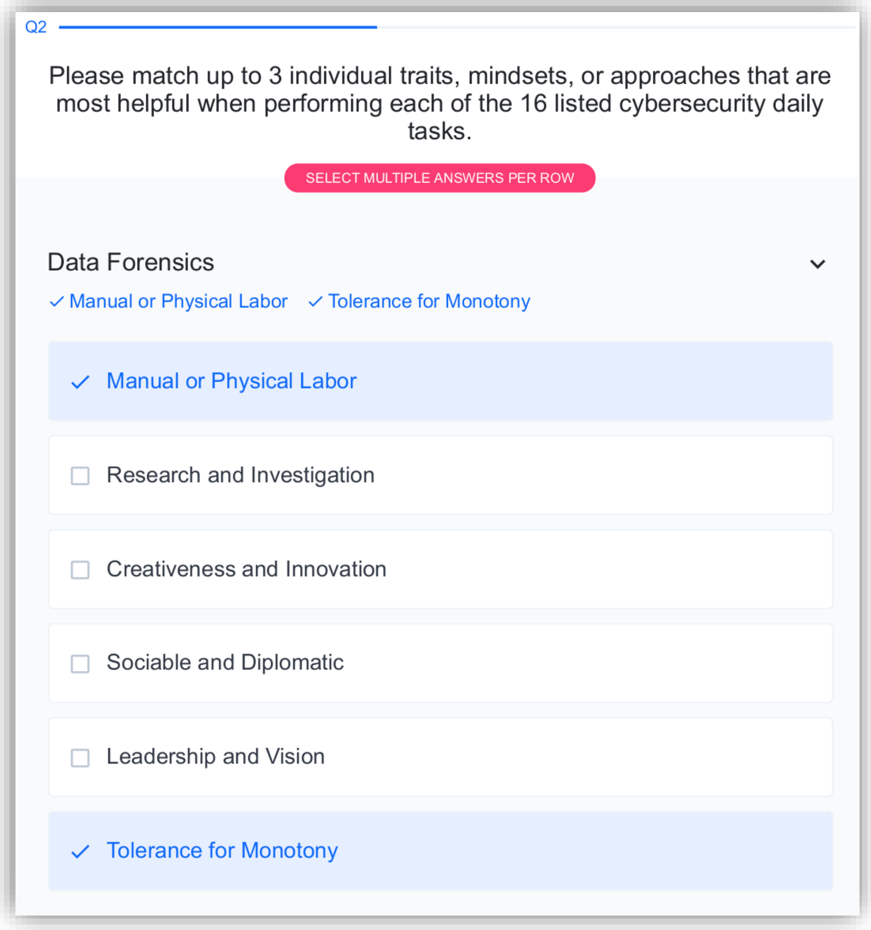
1. My primary job function(s) currently or formerly pertain to cybersecurity as listed in at least one of the cybersecurity job functions below, and I accept the Informed Consent Requirement.

Yes
No

2. Please match up to 3 individual traits, mindsets, or approaches that are most helpful when performing each of the 16 listed cybersecurity daily tasks. (MatrixMultipleSelection)

Row Headings:
Data Forensics
Access Control and Identity Management
Documentation and Cataloging
Physical Security
Intrusion Analysis
Legal and Compliance Investigation
Software Development Security
Management and Coordination

Column Headings:
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony



Please match up to 3 individual traits, mindsets, or approaches that are most helpful when performing each of the 16 listed cybersecurity daily tasks.

Data Forensics

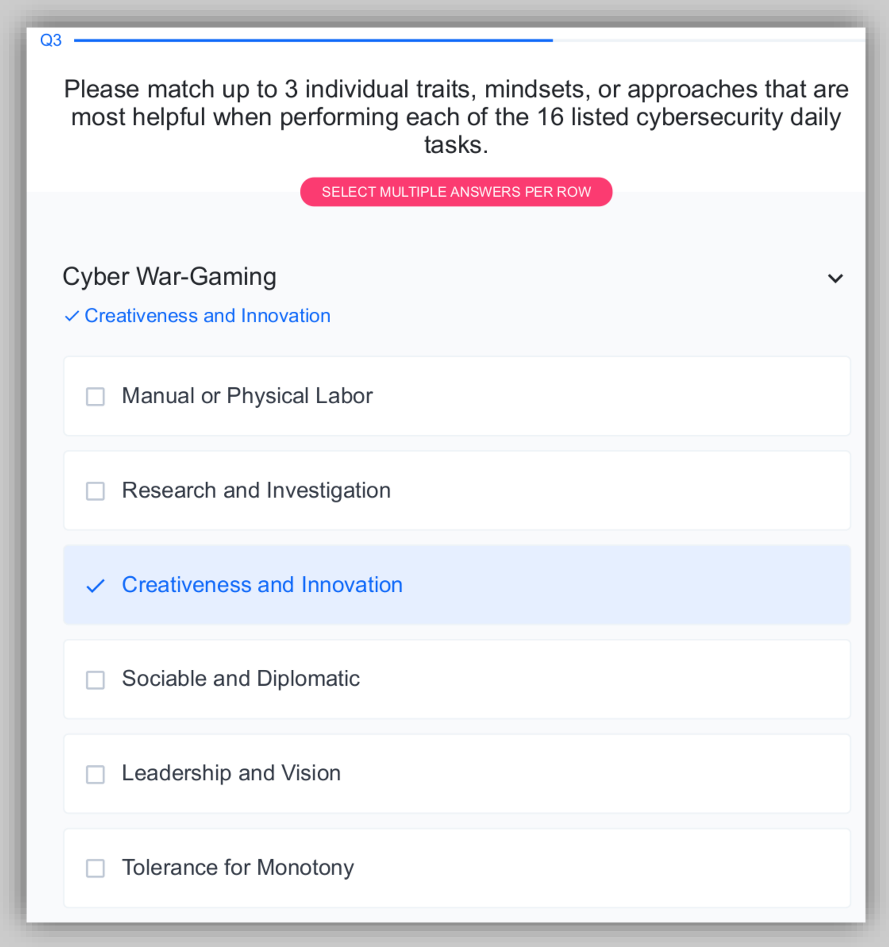
✓ Manual or Physical Labor ✓ Tolerance for Monotony

- ✓ Manual or Physical Labor
- □ Research and Investigation
- □ Creativeness and Innovation
- □ Sociable and Diplomatic
- □ Leadership and Vision
- ✓ Tolerance for Monotony

3. Please match up to 3 individual traits, mindsets, or approaches that are most helpful when performing each of the 16 listed cybersecurity daily tasks. (MatrixMultipleSelection)

Row Headings:
Cyber War-Gaming
Physical Infiltration
Communication and Reporting
Security Training
Risk Management
Social Engineering and Infiltration
Technical Exploitation
Alert Monitoring

Column Headings:
Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony



Please match up to 3 individual traits, mindsets, or approaches that are most helpful when performing each of the 16 listed cybersecurity daily tasks.

Cyber War-Gaming

✓ Creativeness and Innovation

□ Manual or Physical Labor

□ Research and Investigation

✓ Creativeness and Innovation

□ Sociable and Diplomatic

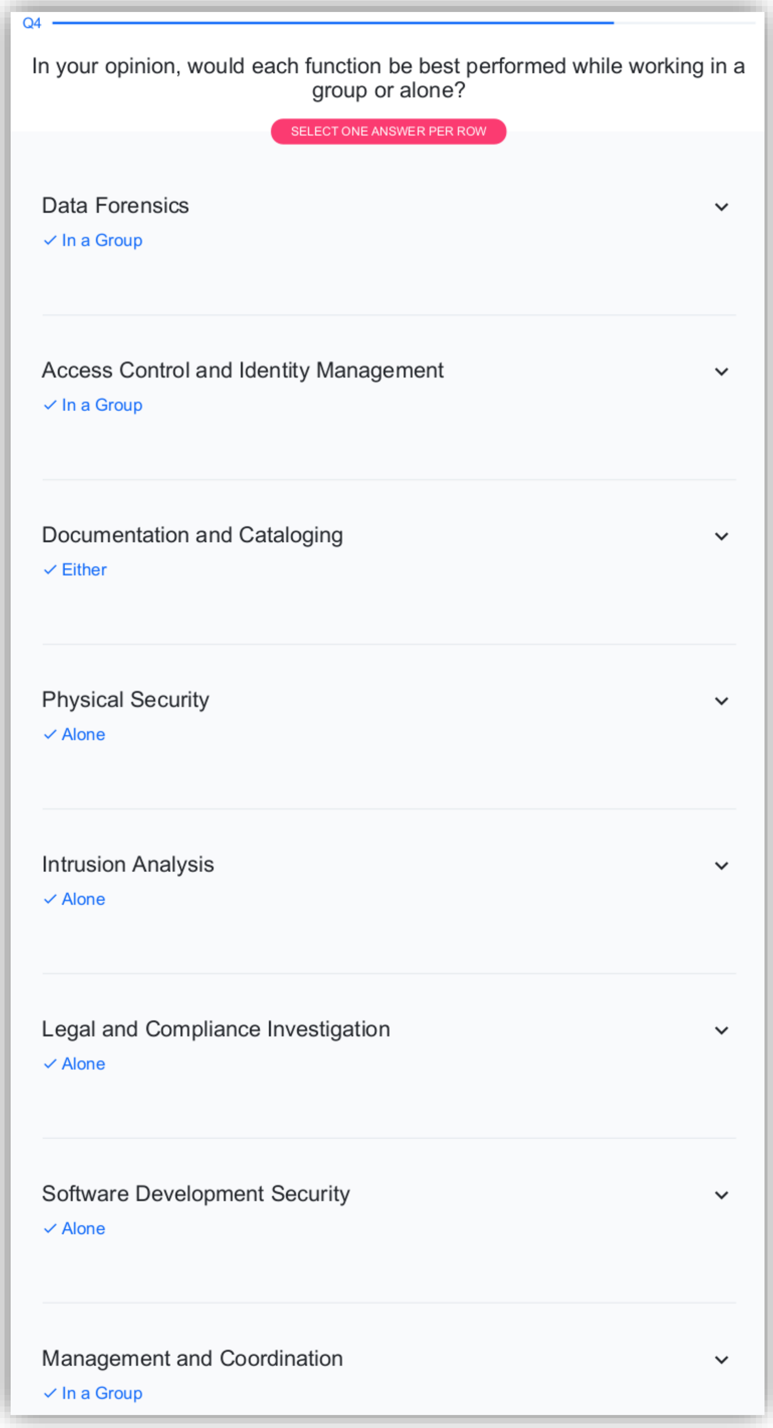
□ Leadership and Vision

□ Tolerance for Monotony

4. In your opinion, would each function be best performed while working in a group or alone? (MatrixSingleSelection)

Row Headings:
Data Forensics
Access Control and Identity Management
Documentation and Cataloging
Physical Security
Intrusion Analysis
Legal and Compliance Investigation
Software Development Security
Management and Coordination

Column Headings:
Alone
In a Group
Either



Q4

In your opinion, would each function be best performed while working in a group or alone?

SELECT ONE ANSWER PER ROW

Data Forensics
✓ In a Group

Access Control and Identity Management
✓ In a Group

Documentation and Cataloging
✓ Either

Physical Security
✓ Alone

Intrusion Analysis
✓ Alone

Legal and Compliance Investigation
✓ Alone

Software Development Security
✓ Alone

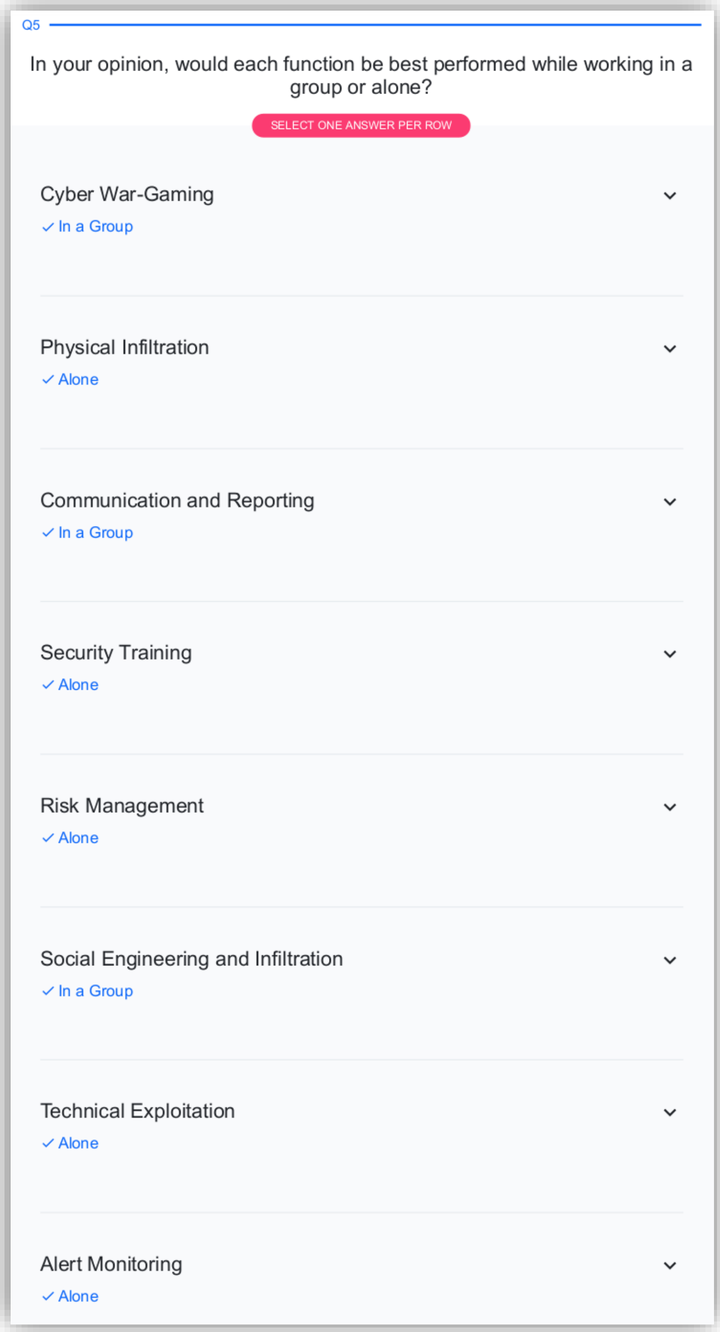
Management and Coordination
✓ In a Group

5. In your opinion, would each function be best performed while working in a group or alone? (MatrixSingleSelection)

Row Headings:
Cyber War-Gaming
Physical Infiltration
Communication and Reporting
Security Training

Risk Management
Social Engineering and Infiltration
Technical Exploitation
Alert Monitoring

Column Headings:
Alone
In a Group
Either



Q5

In your opinion, would each function be best performed while working in a group or alone?

SELECT ONE ANSWER PER ROW

Cyber War-Gaming
✓ In a Group

Physical Infiltration
✓ Alone

Communication and Reporting
✓ In a Group

Security Training
✓ Alone

Risk Management
✓ Alone

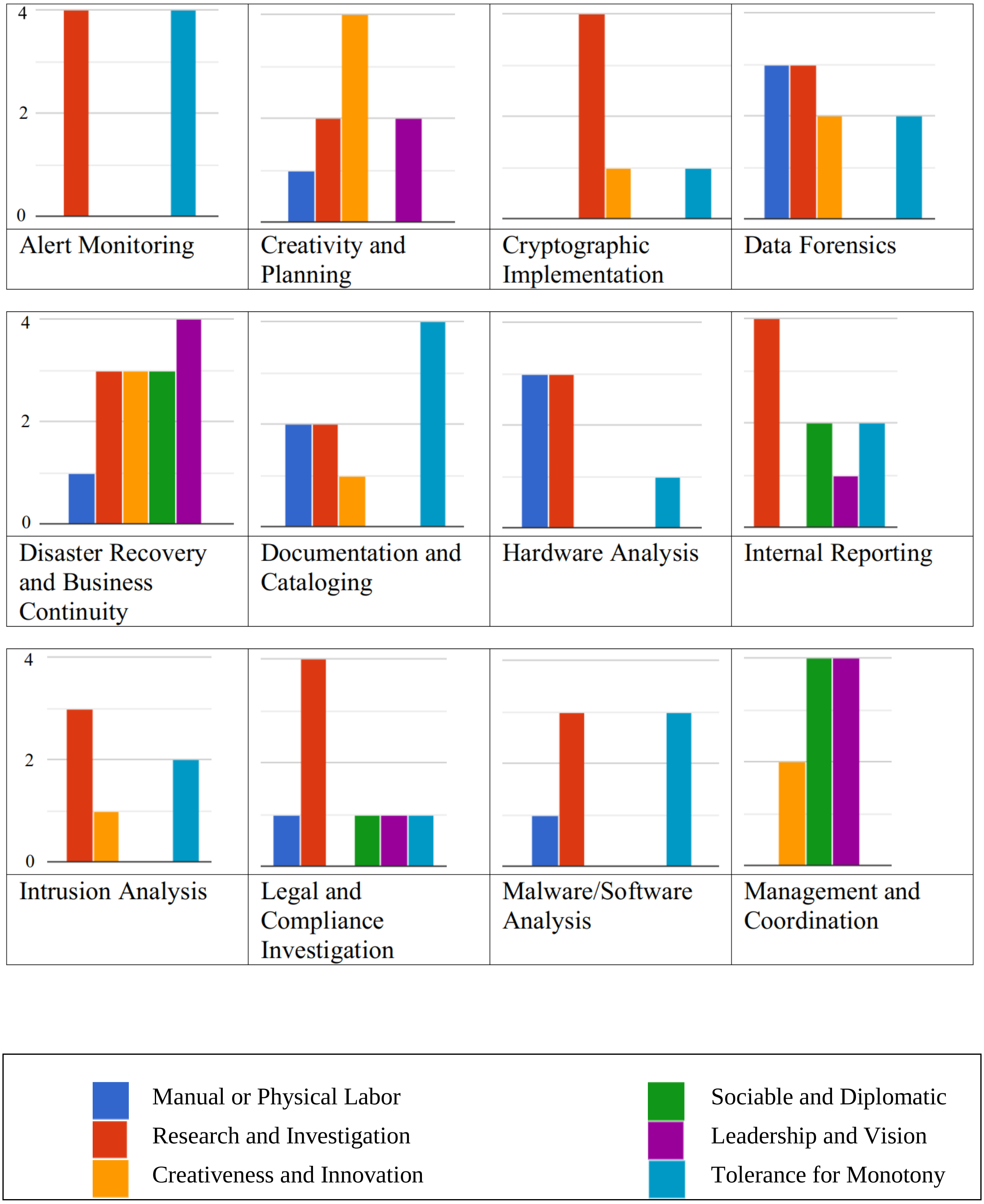
Social Engineering and Infiltration
✓ In a Group

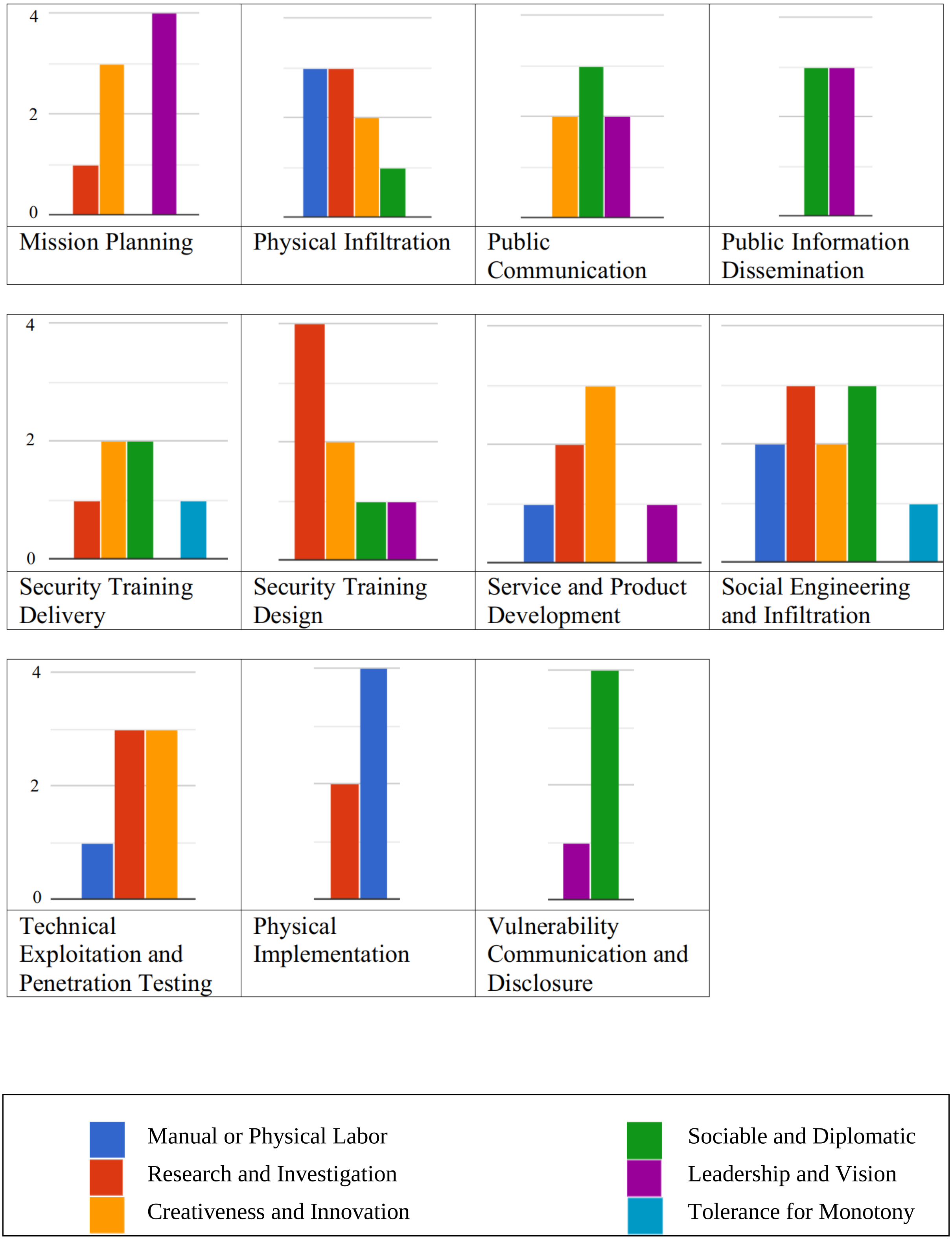
Technical Exploitation
✓ Alone

Alert Monitoring
✓ Alone

D.1 Expert Interview 1 Data

Question 5 – Data Summary





Mission Planning

Physical Infiltration

Public Communication

Public Information Dissemination

Security Training Delivery

Security Training Design

Service and Product Development

Social Engineering and Infiltration

Technical Exploitation and Penetration Testing

Physical Implementation

Vulnerability Communication and Disclosure

D.1 Expert Interview 1 Data

Question 5 – Detailed Responses

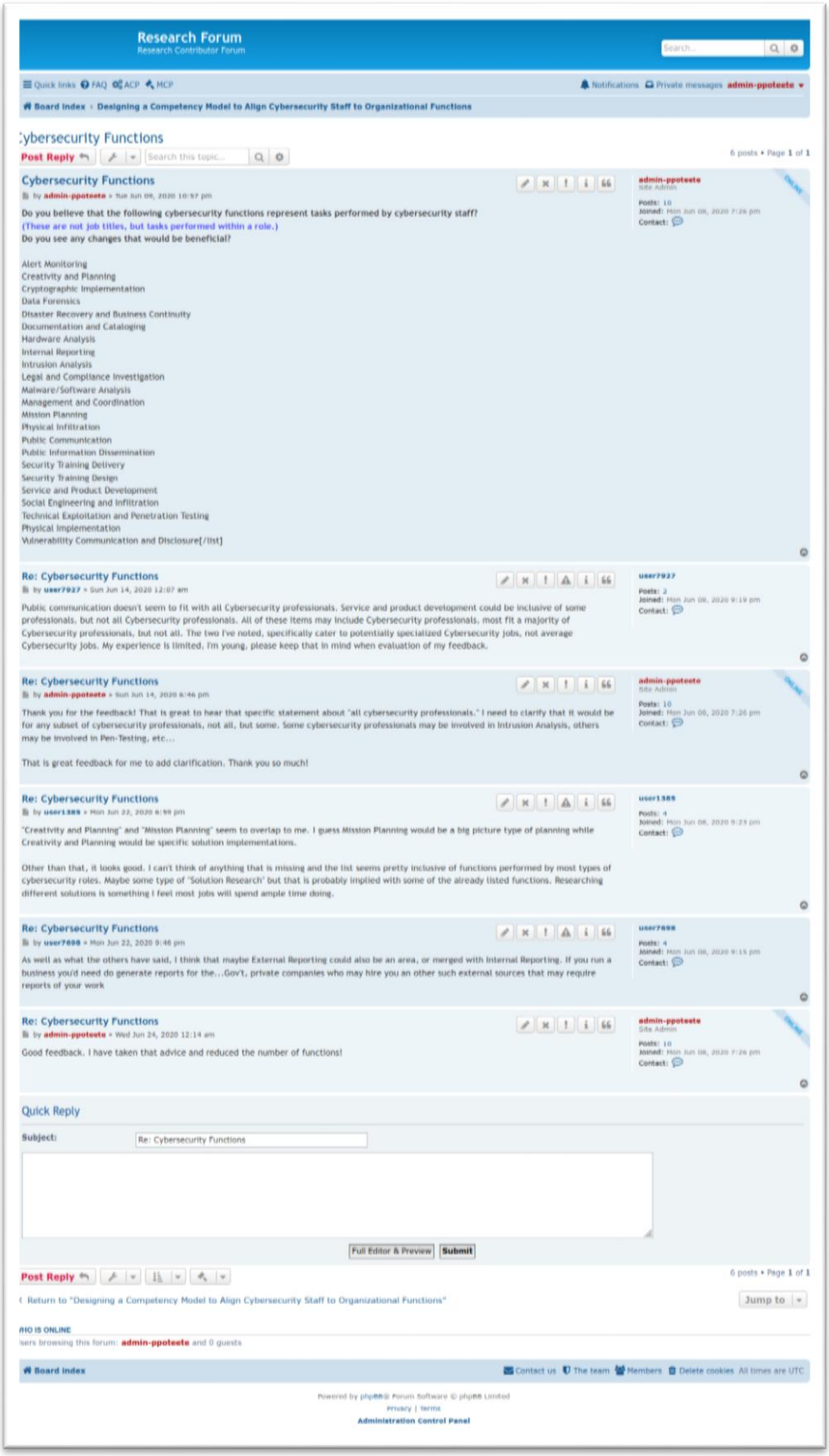
Participant	Alert Monitoring	Creativity and Planning	Cryptographic Implementation	Data Forensics	Disaster Recovery and Business Continuity	Documentation and Cataloging
1	Tolerance for Monotony	Research and Investigation, Creativeness and Innovation	Research and Investigation, Tolerance for Monotony	Research and Investigation, Creativeness and Innovation, Tolerance for Monotony	Manual or Physical Labor, Research and Investigation, Creativeness and Innovation, Sociable and Diplomatic, Leadership and Vision	Tolerance for Monotony
2	Research and Investigation, Tolerance for Monotony	Research and Investigation, Creativeness and Innovation	Research and Investigation, Creativeness and Innovation	Manual or Physical Labor, Research and Investigation, Creativeness and Innovation	Research and Investigation, Creativeness and Innovation, Sociable and Diplomatic, Leadership and Vision	Research and Investigation, Tolerance for Monotony
3	Research and Investigation, Tolerance for Monotony	Creativeness and Innovation, Leadership and Vision	Research and Investigation	Manual or Physical Labor, Research and Investigation	Research and Investigation, Creativeness and Innovation, Leadership and Vision	Research and Investigation, Tolerance for Monotony
4	Research and Investigation	Manual or Physical Labor	no response	Manual or Physical Labor	no response	Manual or Physical Labor
5	Research and Investigation, Tolerance for Monotony	Creativeness and Innovation, Leadership and Vision	Research and Investigation	Tolerance for Monotony	Sociable and Diplomatic, Leadership and Vision	Manual or Physical Labor, Creativeness and Innovation, Tolerance for Monotony

Participant	Hardware Analysis	Internal Reporting	Intrusion Analysis	Legal and Compliance Investigation	Malware/Software Analysis	Management and Coordination
1	Manual or Physical Labor, Tolerance for Monotony	Research and Investigation, Sociable and Diplomatic	Research and Investigation, Creativeness and Innovation	Research and Investigation, Tolerance for Monotony	Research and Investigation, Tolerance for Monotony	Sociable and Diplomatic, Leadership and Vision
2	Manual or Physical Labor, Research and Investigation	Research and Investigation, Tolerance for Monotony	Research and Investigation, Tolerance for Monotony	Research and Investigation, Sociable and Diplomatic	Research and Investigation, Tolerance for Monotony	Sociable and Diplomatic, Leadership and Vision
3	Manual or Physical Labor	Research and Investigation, Sociable and Diplomatic, Leadership and Vision	Research and Investigation	Research and Investigation	Research and Investigation	Creativeness and Innovation, Sociable and Diplomatic, Leadership and Vision
4	Research and Investigation	no response	no response	no response	Manual or Physical Labor	no response
5	Research and Investigation	Research and Investigation, Tolerance for Monotony	Tolerance for Monotony	Manual or Physical Labor, Research and Investigation, Leadership and Vision	Tolerance for Monotony	Creativeness and Innovation, Sociable and Diplomatic, Leadership and Vision

Participant	Mission Planning	Physical Infiltration	Public Communication	Public Information Dissemination	Security Training Delivery	Security Training Design
1	Creativeness and Innovation, Leadership and Vision	Manual or Physical Labor, Creativeness and Innovation	Sociable and Diplomatic	Sociable and Diplomatic	Sociable and Diplomatic	Research and Investigation
2	Research and Investigation, Leadership and Vision	Manual or Physical Labor, Research and Investigation	Sociable and Diplomatic, Leadership and Vision	Sociable and Diplomatic, Leadership and Vision	Sociable and Diplomatic, Tolerance for Monotony	Research and Investigation, Sociable and Diplomatic
3	Creativeness and Innovation, Leadership and Vision	Manual or Physical Labor, Research and Investigation	Creativeness and Innovation, Sociable and Diplomatic, Leadership and Vision	Sociable and Diplomatic, Leadership and Vision	Research and Investigation, Creativeness and Innovation	Research and Investigation, Creativeness and Innovation, Leadership and Vision
4	no response	no response	no response	no response	no response	no response
5	Creativeness and Innovation, Leadership and Vision	Research and Investigation, Creativeness and Innovation, Sociable and Diplomatic	Creativeness and Innovation	Leadership and Vision	Creativeness and Innovation	Research and Investigation, Creativeness and Innovation

Participant	Service and Product Development	Social Engineering and Infiltration	Technical Exploitation and Penetration Testing	Physical Implementation	Vulnerability Communication and Disclosure
1	Creativeness and Innovation	Manual or Physical Labor, Creativeness and Innovation, Sociable and Diplomatic	Research and Investigation, Creativeness and Innovation	Manual or Physical Labor	Sociable and Diplomatic
2	Research and Investigation, Creativeness and Innovation	Research and Investigation, Sociable and Diplomatic	Research and Investigation, Creativeness and Innovation	Manual or Physical Labor, Research and Investigation	Sociable and Diplomatic
3	Creativeness and Innovation	Research and Investigation	Manual or Physical Labor, Research and Investigation	Manual or Physical Labor	Sociable and Diplomatic
4	no response	no response	no response	no response	no response
5	Manual or Physical Labor, Research and Investigation, Leadership and Vision	Manual or Physical Labor, Research and Investigation, Creativeness and Innovation, Sociable and Diplomatic, Tolerance for Monotony	Creativeness and Innovation	Manual or Physical Labor, Research and Investigation	Sociable and Diplomatic, Leadership and Vision

D.2 Focus Group Data



Research Forum
Research Contributor Forum
Search...
Quick links FAQ ACP MCP
Notifications Private messages admin-ppoteete
Board index ‹ Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions

:ybersecurity Functions

Post Reply
Search this topic...
6 posts • Page 1 of 1

Cybersecurity Functions

by admin-ppoteete » Tue Jun 09, 2020 10:57 pm

admin-ppoteete
Site Admin
Posts: 10
Joined: Mon Jun 08, 2020 7:26 pm
Contact:

Do you believe that the following cybersecurity functions represent tasks performed by cybersecurity staff?
(These are not job titles, but tasks performed within a role.)
Do you see any changes that would be beneficial?

Alert Monitoring
Creativity and Planning
Cryptographic Implementation
Data Forensics
Disaster Recovery and Business Continuity
Documentation and Cataloging
Hardware Analysis
Internal Reporting
Intrusion Analysis
Legal and Compliance Investigation
Malware/Software Analysis
Management and Coordination
Mission Planning
Physical Infiltration
Public Communication
Public Information Dissemination
Security Training Delivery
Security Training Design
Service and Product Development
Social Engineering and Infiltration
Technical Exploitation and Penetration Testing
Physical Implementation
Vulnerability Communication and Disclosure[/list]

Re: Cybersecurity Functions

by user7927 » Sun Jun 14, 2020 12:07 am

user7927
Posts: 2
Joined: Mon Jun 08, 2020 9:19 pm
Contact:

Public communication doesn't seem to fit with all Cybersecurity professionals. Service and product development could be inclusive of some professionals, but not all Cybersecurity professionals. All of these items may include Cybersecurity professionals, most fit a majority of Cybersecurity professionals, but not all. The two I've noted, specifically cater to potentially specialized Cybersecurity jobs, not average Cybersecurity jobs. My experience is limited, I'm young, please keep that in mind when evaluation of my feedback.

Re: Cybersecurity Functions

by admin-ppoteete » Sun Jun 14, 2020 6:46 pm

admin-ppoteete
Site Admin
Posts: 10
Joined: Mon Jun 08, 2020 7:26 pm
Contact:

Thank you for the feedback! That is great to hear that specific statement about "all cybersecurity professionals." I need to clarify that it would be for any subset of cybersecurity professionals, not all, but some. Some cybersecurity professionals may be involved in Intrusion Analysis, others may be involved in Pen-Testing, etc...

That is great feedback for me to add clarification. Thank you so much!

Re: Cybersecurity Functions

by user1385 » Mon Jun 22, 2020 6:59 pm

user1385
Posts: 4
Joined: Mon Jun 08, 2020 9:23 pm
Contact:

"Creativity and Planning" and "Mission Planning" seem to overlap to me. I guess Mission Planning would be a big picture type of planning while Creativity and Planning would be specific solution implementations.

Other than that, it looks good. I can't think of anything that is missing and the list seems pretty inclusive of functions performed by most types of cybersecurity roles. Maybe some type of "Solution Research" but that is probably implied with some of the already listed functions. Researching different solutions is something I feel most jobs will spend ample time doing.

Re: Cybersecurity Functions

by user7698 » Mon Jun 22, 2020 9:46 pm

user7698
Posts: 4
Joined: Mon Jun 08, 2020 9:15 pm
Contact:

As well as what the others have said, I think that maybe External Reporting could also be an area, or merged with Internal Reporting. If you run a business you'd need do generate reports for the...Gov't, private companies who may hire you an other such external sources that may require reports of your work

Re: Cybersecurity Functions

by admin-ppoteete » Wed Jun 24, 2020 12:14 am

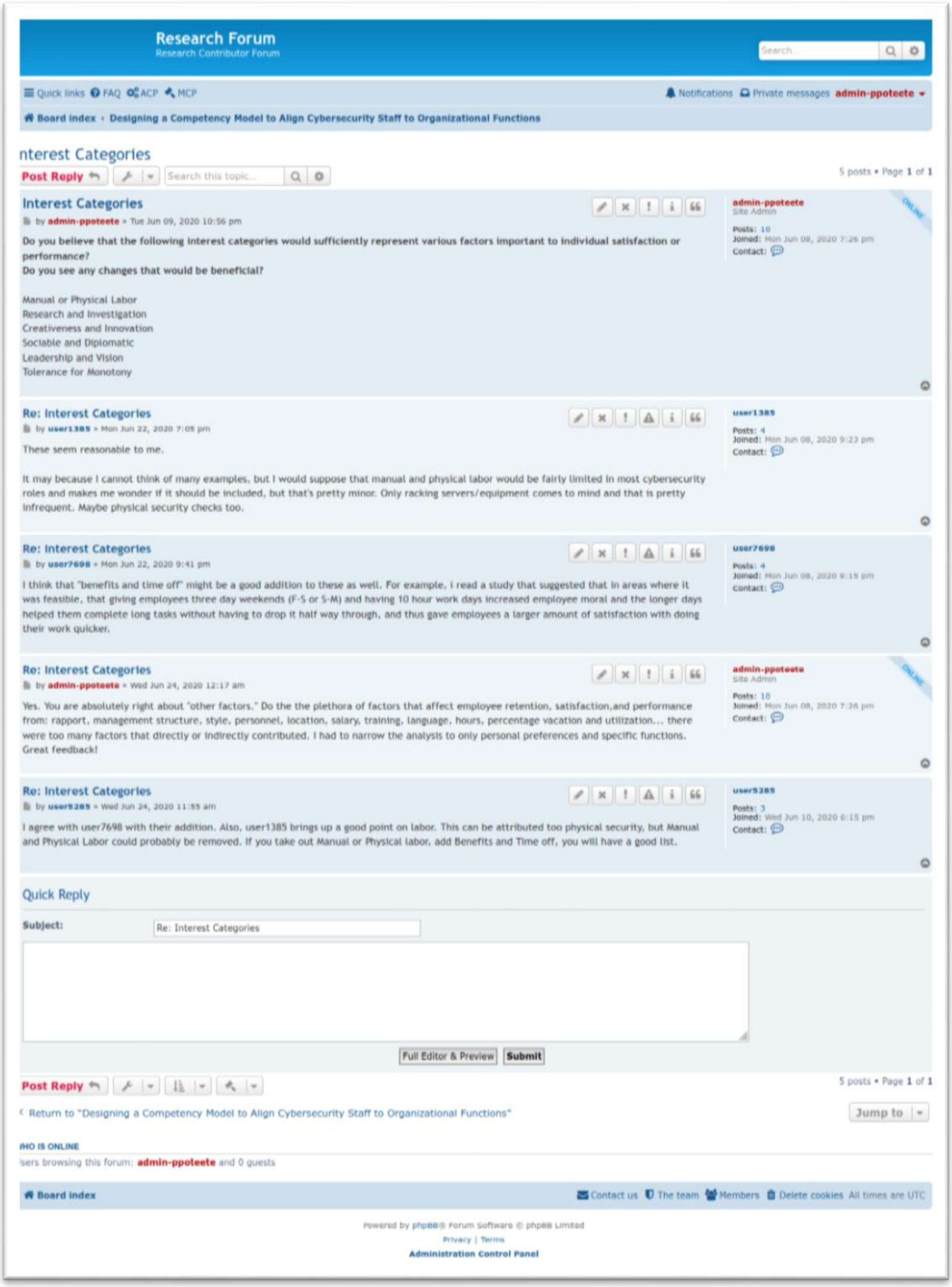
admin-ppoteete
Site Admin
Posts: 10
Joined: Mon Jun 08, 2020 7:26 pm
Contact:

Good feedback. I have taken that advice and reduced the number of functions!

Quick Reply

Subject: Re: Cybersecurity Functions

Full Editor & Preview
Submit
Post Reply
6 posts • Page 1 of 1
‹ Return to "Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions"
Jump to
WHO IS ONLINE
Users browsing this forum: admin-ppoteete and 0 guests
Board index
Contact us
The team
Members
Delete cookies
All times are UTC
Powered by phpBB® Forum Software © phpBB Limited
Privacy | Terms
Administration Control Panel



Interest Categories
by admin-ppoteete » Tue Jun 09, 2020 10:56 pm

Do you believe that the following interest categories would sufficiently represent various factors important to individual satisfaction or performance?
Do you see any changes that would be beneficial?

Manual or Physical Labor
Research and Investigation
Creativeness and Innovation
Sociable and Diplomatic
Leadership and Vision
Tolerance for Monotony

admin-ppoteete
Site Admin
Posts: 10
Joined: Mon Jun 08, 2020 7:26 pm
Contact:

Re: Interest Categories
by user1385 » Mon Jun 22, 2020 7:05 pm

These seem reasonable to me.

It may because I cannot think of many examples, but I would suppose that manual and physical labor would be fairly limited in most cybersecurity roles and makes me wonder if it should be included, but that's pretty minor. Only racking servers/equipment comes to mind and that is pretty infrequent. Maybe physical security checks too.

user1385
Posts: 4
Joined: Mon Jun 08, 2020 9:23 pm
Contact:

Re: Interest Categories
by user7698 » Mon Jun 22, 2020 9:41 pm

I think that "benefits and time off" might be a good addition to these as well. For example, I read a study that suggested that in areas where it was feasible, that giving employees three day weekends (F-S or S-M) and having 10 hour work days increased employee moral and the longer days helped them complete long tasks without having to drop it half way through, and thus gave employees a larger amount of satisfaction with doing their work quicker.

user7698
Posts: 4
Joined: Mon Jun 08, 2020 9:15 pm
Contact:

Re: Interest Categories
by admin-ppoteete » Wed Jun 24, 2020 12:17 am

Yes. You are absolutely right about "other factors." Do the the plethora of factors that affect employee retention, satisfaction,and performance from: rapport, management structure, style, personnel, location, salary, training, language, hours, percentage vacation and utilization... there were too many factors that directly or indirectly contributed. I had to narrow the analysis to only personal preferences and specific functions. Great feedback!

admin-ppoteete
Site Admin
Posts: 10
Joined: Mon Jun 08, 2020 7:26 pm
Contact:

Re: Interest Categories
by user5285 » Wed Jun 24, 2020 11:55 am

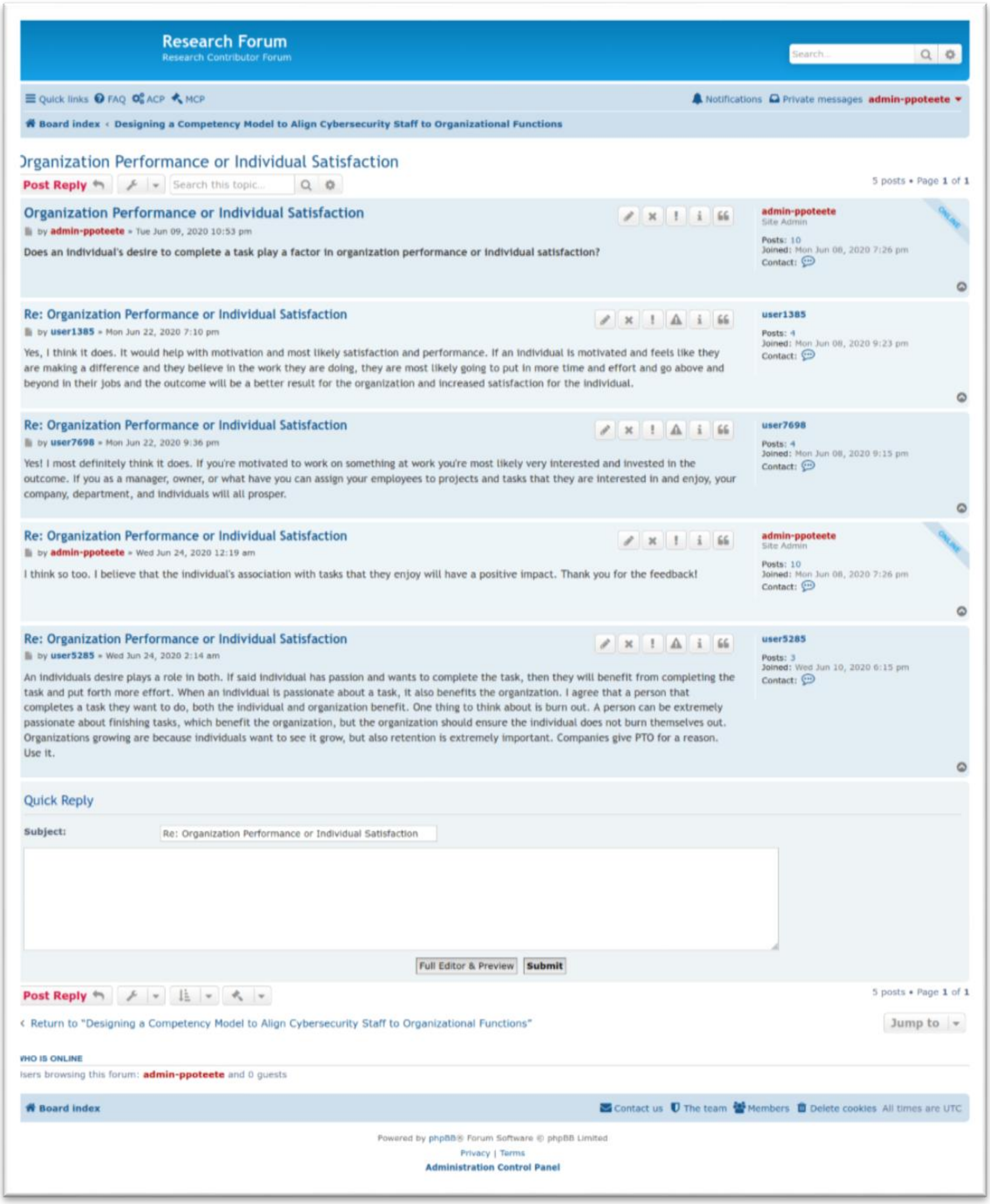
I agree with user7698 with their addition. Also, user1385 brings up a good point on labor. This can be attributed too physical security, but Manual and Physical Labor could probably be removed. If you take out Manual or Physical labor, add Benefits and Time off, you will have a good list.

user5285
Posts: 3
Joined: Wed Jun 10, 2020 6:15 pm
Contact:

Quick Reply

Subject: Re: Interest Categories

Full Editor & Preview
Submit
Post Reply
5 posts • Page 1 of 1
‹ Return to "Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions"
Jump to
WHO IS ONLINE
sers browsing this forum: admin-ppoteete and 0 guests
Board index
Contact us
The team
Members
Delete cookies
All times are UTC
Powered by phpBB® Forum Software © phpBB Limited
Privacy | Terms
Administration Control Panel



Drganization Performance or Individual Satisfaction

Organization Performance or Individual Satisfaction
by admin-ppoteete » Tue Jun 09, 2020 10:53 pm

Does an individual's desire to complete a task play a factor in organization performance or individual satisfaction?

admin-ppoteete
Site Admin
Posts: 10
Joined: Mon Jun 08, 2020 7:26 pm
Contact:

Re: Organization Performance or Individual Satisfaction
by user1385 » Mon Jun 22, 2020 7:10 pm

Yes, I think it does. It would help with motivation and most likely satisfaction and performance. If an individual is motivated and feels like they are making a difference and they believe in the work they are doing, they are most likely going to put in more time and effort and go above and beyond in their jobs and the outcome will be a better result for the organization and increased satisfaction for the individual.

user1385
Posts: 4
Joined: Mon Jun 08, 2020 9:23 pm
Contact:

Re: Organization Performance or Individual Satisfaction
by user7698 » Mon Jun 22, 2020 9:36 pm

Yes! I most definitely think it does. If you're motivated to work on something at work you're most likely very interested and invested in the outcome. If you as a manager, owner, or what have you can assign your employees to projects and tasks that they are interested in and enjoy, your company, department, and individuals will all prosper.

user7698
Posts: 4
Joined: Mon Jun 08, 2020 9:15 pm
Contact:

Re: Organization Performance or Individual Satisfaction
by admin-ppoteete » Wed Jun 24, 2020 12:19 am

I think so too. I believe that the individual's association with tasks that they enjoy will have a positive impact. Thank you for the feedback!

admin-ppoteete
Site Admin
Posts: 10
Joined: Mon Jun 08, 2020 7:26 pm
Contact:

Re: Organization Performance or Individual Satisfaction
by user5285 » Wed Jun 24, 2020 2:14 am

An individuals desire plays a role in both. If said individual has passion and wants to complete the task, then they will benefit from completing the task and put forth more effort. When an individual is passionate about a task, it also benefits the organization. I agree that a person that completes a task they want to do, both the individual and organization benefit. One thing to think about is burn out. A person can be extremely passionate about finishing tasks, which benefit the organization, but the organization should ensure the individual does not burn themselves out. Organizations growing are because individuals want to see it grow, but also retention is extremely important. Companies give PTO for a reason. Use it.

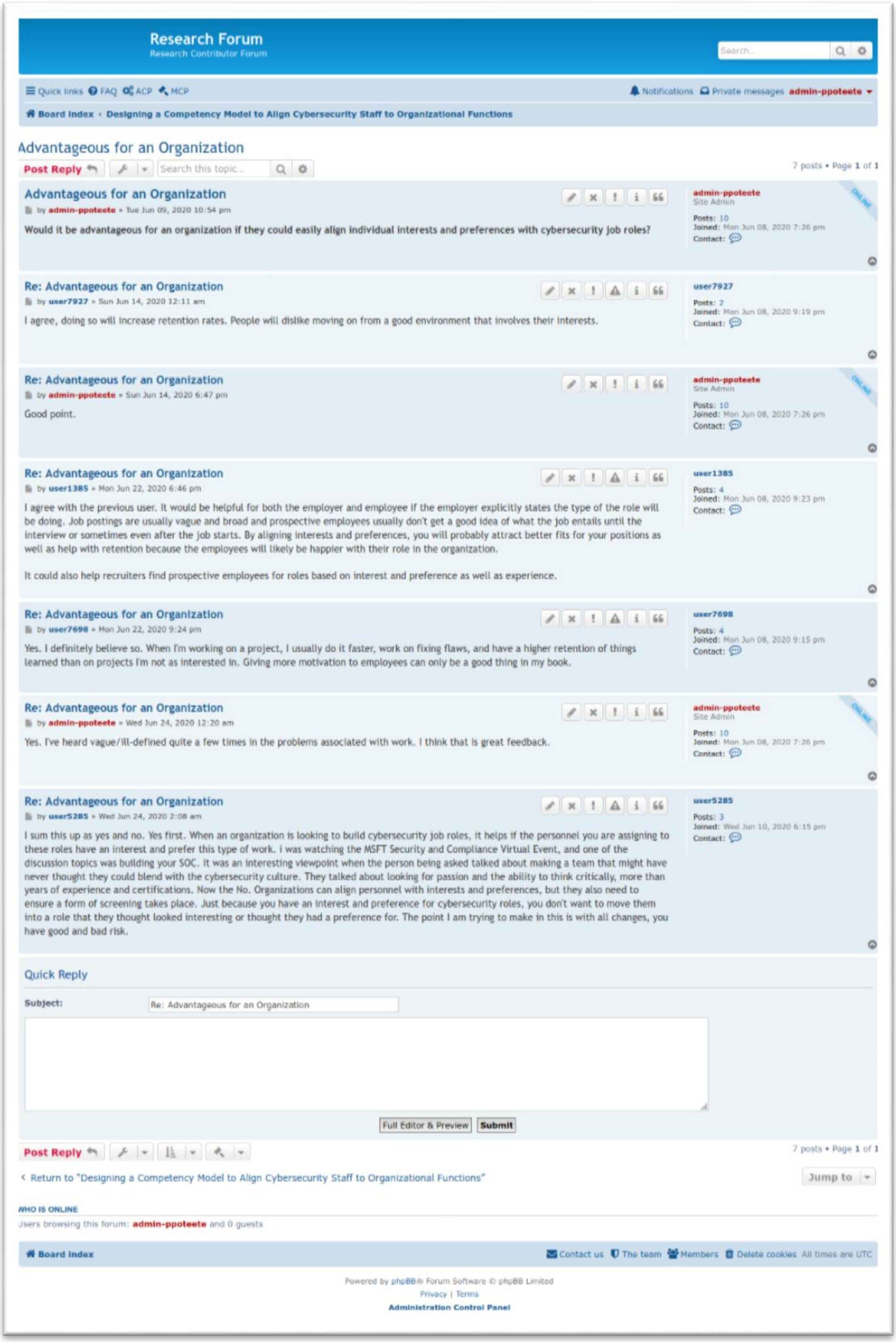
user5285
Posts: 3
Joined: Wed Jun 10, 2020 6:15 pm
Contact:

Quick Reply

Subject: Re: Organization Performance or Individual Satisfaction

Full Editor & Preview
Submit
Post Reply
5 posts • Page 1 of 1
‹ Return to "Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions"
Jump to
VHO IS ONLINE

Isers browsing this forum: admin-ppoteete and 0 guests



Advantageous for an Organization

Advantageous for an Organization
by admin-ppoteete » Tue Jun 09, 2020 10:54 pm

Would it be advantageous for an organization if they could easily align individual interests and preferences with cybersecurity job roles?

admin-ppoteete
Site Admin
Posts: 10
Joined: Mon Jun 08, 2020 7:26 pm
Contact:

Re: Advantageous for an Organization
by user7927 » Sun Jun 14, 2020 12:11 am

I agree, doing so will increase retention rates. People will dislike moving on from a good environment that involves their interests.

user7927
Posts: 2
Joined: Mon Jun 08, 2020 9:19 pm
Contact:

Re: Advantageous for an Organization
by admin-ppoteete » Sun Jun 14, 2020 6:47 pm

Good point.

admin-ppoteete
Site Admin
Posts: 10
Joined: Mon Jun 08, 2020 7:26 pm
Contact:

Re: Advantageous for an Organization
by user1385 » Mon Jun 22, 2020 6:46 pm

I agree with the previous user. It would be helpful for both the employer and employee if the employer explicitly states the type of the role will be doing. Job postings are usually vague and broad and prospective employees usually don't get a good idea of what the job entails until the interview or sometimes even after the job starts. By aligning interests and preferences, you will probably attract better fits for your positions as well as help with retention because the employees will likely be happier with their role in the organization.

It could also help recruiters find prospective employees for roles based on interest and preference as well as experience.

user1385
Posts: 4
Joined: Mon Jun 08, 2020 9:23 pm
Contact:

Re: Advantageous for an Organization
by user7698 » Mon Jun 22, 2020 9:24 pm

Yes. I definitely believe so. When I'm working on a project, I usually do it faster, work on fixing flaws, and have a higher retention of things learned than on projects I'm not as interested in. Giving more motivation to employees can only be a good thing in my book.

user7698
Posts: 4
Joined: Mon Jun 08, 2020 9:15 pm
Contact:

Re: Advantageous for an Organization
by admin-ppoteete » Wed Jun 24, 2020 12:20 am

Yes. I've heard vague/ill-defined quite a few times in the problems associated with work. I think that is great feedback.

admin-ppoteete
Site Admin
Posts: 10
Joined: Mon Jun 08, 2020 7:26 pm
Contact:

Re: Advantageous for an Organization
by user5285 » Wed Jun 24, 2020 2:08 am

I sum this up as yes and no. Yes first. When an organization is looking to build cybersecurity job roles, it helps if the personnel you are assigning to these roles have an interest and prefer this type of work. i was watching the MSFT Security and Compliance Virtual Event, and one of the discussion topics was building your SOC. It was an interesting viewpoint when the person being asked talked about making a team that might have never thought they could blend with the cybersecurity culture. They talked about looking for passion and the ability to think critically, more than years of experience and certifications. Now the No. Organizations can align personnel with interests and preferences, but they also need to ensure a form of screening takes place. Just because you have an interest and preference for cybersecurity roles, you don't want to move them into a role that they thought looked interesting or thought they had a preference for. The point I am trying to make in this is with all changes, you have good and bad risk.

user5285
Posts: 3
Joined: Wed Jun 10, 2020 6:15 pm
Contact:

Quick Reply

Subject: Re: Advantageous for an Organization

Full Editor & Preview
Submit
Post Reply
7 posts • Page 1 of 1
Return to "Designing a Competency Model to Align Cybersecurity Staff to Organizational Functions"
Jump to
WHO IS ONLINE
Users browsing this forum: admin-ppoteete and 0 guests
Board index
Contact us
The team
Members
Delete cookies
All times are UTC
Powered by phpBB® Forum Software © phpBB Limited
Privacy | Terms
Administration Control Panel

D.2 Focus Group Data

Topic: Cybersecurity Functions

"Public communication doesn't seem to fit with all Cybersecurity professionals. Service and product development could be inclusive of some professionals, but not all Cybersecurity professionals. All of these items may include Cybersecurity professionals, most fit a majority of Cybersecurity professionals, but not all. The two I've noted, specifically cater to potentially specialized Cybersecurity jobs, not average Cybersecurity jobs. My experience is limited, I'm young, please keep that in mind when evaluation of my feedback."

"Creativity and Planning and Mission Planning seem to overlap to me. I guess Mission Planning would be a big picture type of planning while Creativity and Planning would be specific solution implementations. Other than that, it looks good. I can't think of anything that is missing and the list seems pretty inclusive of functions performed by most types of cybersecurity roles. Maybe some type of Solution Research but that is probably implied with some of the already listed functions. Researching different solutions is something I feel most jobs will spend ample time doing."

"As well as what the others have said, I think that maybe External Reporting could also be an area, or merged with Internal Reporting. If you run a business you'd need do generate reports for the...Gov't, private companies who may hire you an other such external sources that may require reports of your work."

Topic: Interest Categories

"These seem reasonable to me. It may because I cannot think of many examples, but I would suppose that manual and physical labor would be fairly limited in most cybersecurity roles and makes me wonder if it should be included, but that's pretty minor. Only racking servers/equipment comes to mind and that is pretty infrequent. Maybe physical security checks too."

"I think that "benefits and time off" might be a good addition to these as well. For example, I read a study that suggested that in areas where it was feasible, that giving employees three day weekends (F-S or S-M) and having 10 hour work days increased employee moral and the longer days helped them complete long tasks without having to drop it half way through, and thus gave employees a larger amount of satisfaction with doing their work quicker."

"I agree with user7698 with their addition. Also, user1385 brings up a good point on labor. This can be attributed too physical security, but Manual and Physical Labor could probably be removed. If you take out Manual or Physical labor, add Benefits and Time off, you will have a good list."

Topic: Organization Performance or Individual Satisfaction

"Yes, I think it does. It would help with motivation and most likely satisfaction and performance. If an individual is motivated and feels like they are making a difference and they believe in the work they are doing, they are most likely going to put in more time and effort and go above and beyond in their jobs and the outcome will be a better result for the organization and increased satisfaction for the individual."

"Yes! I most definitely think it does. If you're motivated to work on something at work you're most likely very interested and invested in the outcome. If you as a manager, owner, or what have you can assign your employees to projects and tasks that they are interested in and enjoy, your company, department, and individuals will all prosper."

"An individuals desire plays a role in both. If said individual has passion and wants to complete the task, then they will benefit from completing the task and put forth more effort. When an individual is passionate about a task, it also benefits the organization. I agree that a person that completes a task they want to do, both the individual and organization benefit. One thing to think about is burn out. A person can be extremely passionate about finishing tasks, which benefit the organization, but the organization should ensure the individual does not burn themselves out. Organizations growing are because individuals want to see it grow, but also retention is extremely important. Companies give PTO for a reason. Use it."

Topic: Advantageous for an Organization

"I agree, doing so will increase retention rates. People will dislike moving on from a good environment that involves their interests."

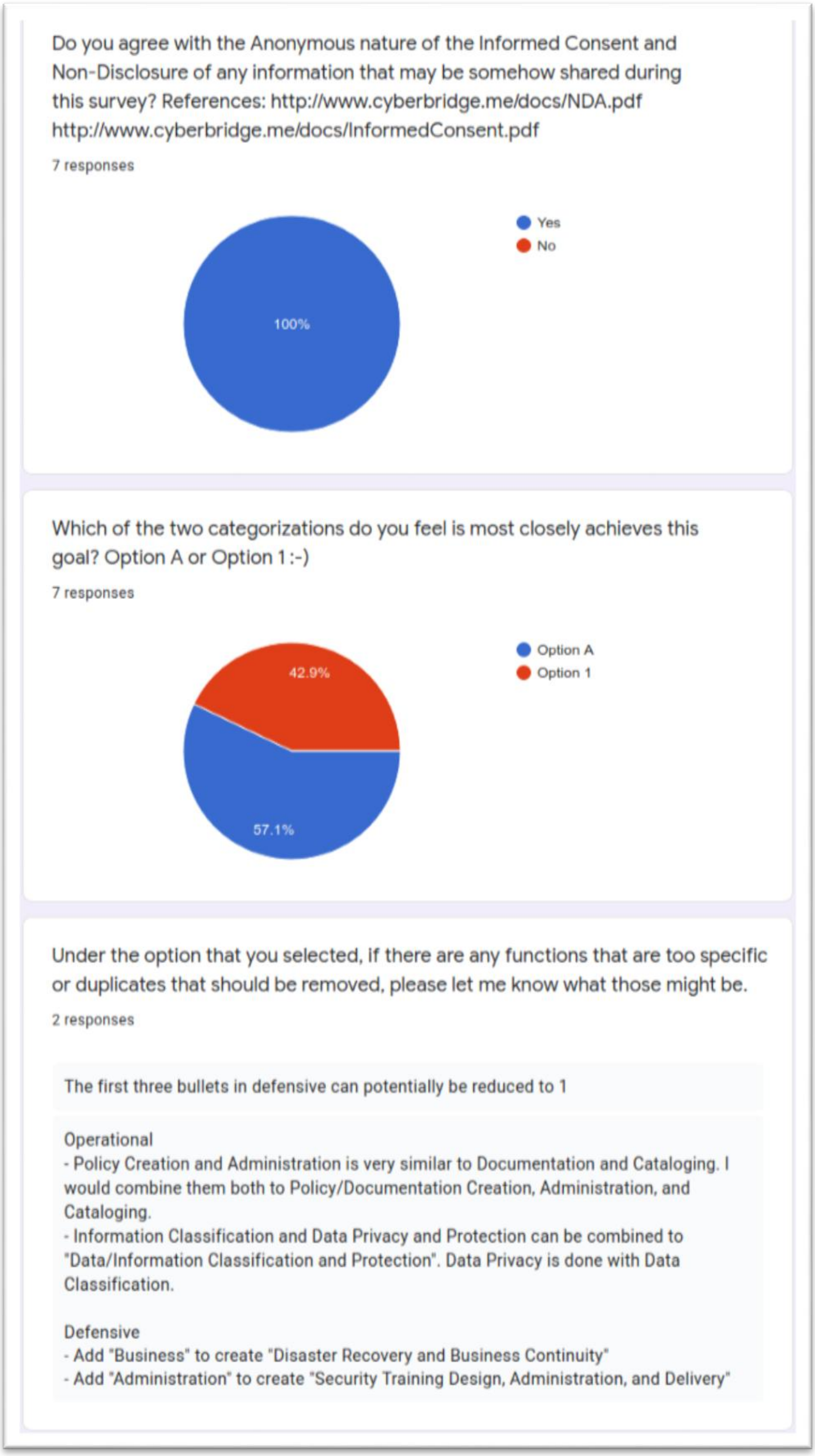
"I agree with the previous user. It would be helpful for both the employer and employee if the employer explicitly states the type of the role will be doing. Job postings are usually vague and broad and prospective employees usually don't get a good idea of what the job entails until the interview or sometimes even after the job starts. By aligning interests and preferences, you will probably attract better fits for your positions as well as help with retention because the employees will likely be happier with their role in the organization. It could also help recruiters find prospective employees for roles based on interest and preference as well as experience."

"Yes. I definitely believe so. When I'm working on a project, I usually do it faster, work on fixing flaws, and have a higher retention of things learned than on projects I'm not as interested in. Giving more motivation to employees can only be a good thing in my book."

"Yes. I've heard vague/ill-defined quite a few times in the problems associated with work. I think that is great feedback."

"I sum this up as yes and no. Yes first. When an organization is looking to build cybersecurity job roles, it helps if the personnel you are assigning to these roles have an interest and prefer this type of work. I was watching the MSFT Security and Compliance Virtual Event, and one of the discussion topics was building your SOC. It was an interesting viewpoint when the person being asked talked about making a team that might have never thought they could blend with the cybersecurity culture. They talked about looking for passion and the ability to think critically, more than years of experience and certifications. Now the No. Organizations can align personnel with interests and preferences, but they also need to ensure a form of screening takes place. Just because you have an interest and preference for cybersecurity roles, you don't want to move them into a role that they thought looked interesting or thought they had a preference for. The point I am trying to make in this is with all changes, you have good and bad risk."

D.3 Job Functions Survey Data



Do you agree with the Anonymous nature of the Informed Consent and Non-Disclosure of any information that may be somehow shared during this survey? References: http://www.cyberbridge.me/docs/NDA.pdf http://www.cyberbridge.me/docs/InformedConsent.pdf

7 responses

Which of the two categorizations do you feel is most closely achieves this goal? Option A or Option 1 :-)

7 responses

Under the option that you selected, if there are any functions that are too specific or duplicates that should be removed, please let me know what those might be.

2 responses

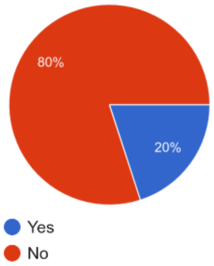
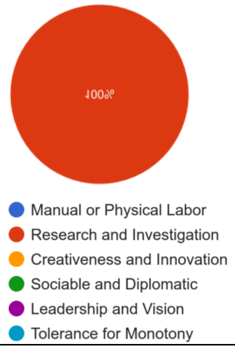
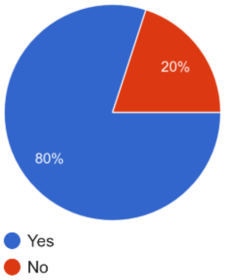
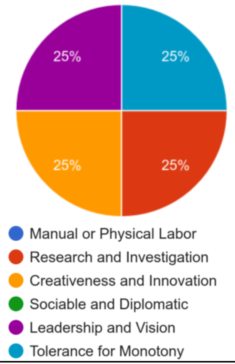
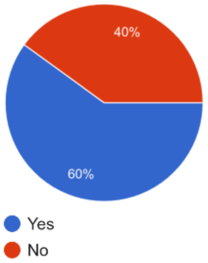
The first three bullets in defensive can potentially be reduced to 1

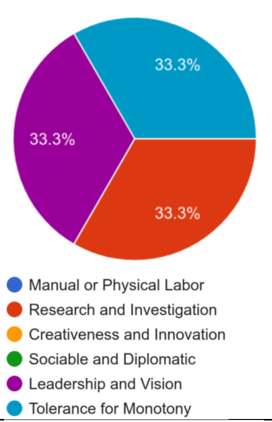
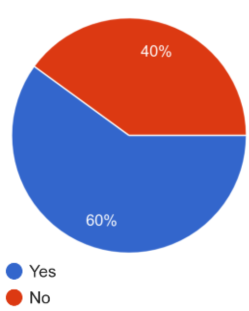
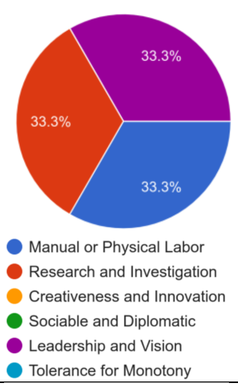
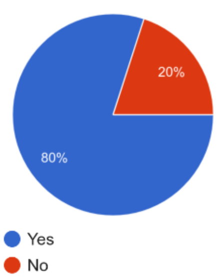
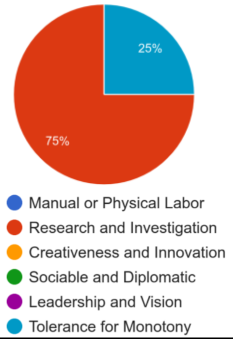
Operational
- Policy Creation and Administration is very similar to Documentation and Cataloging. I would combine them both to Policy/Documentation Creation, Administration, and Cataloging.
- Information Classification and Data Privacy and Protection can be combined to "Data/Information Classification and Protection". Data Privacy is done with Data Classification.

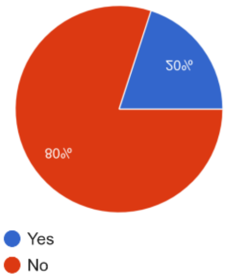
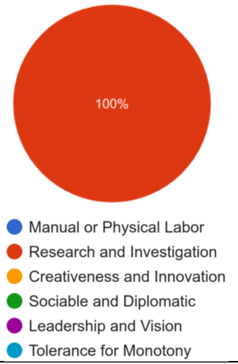
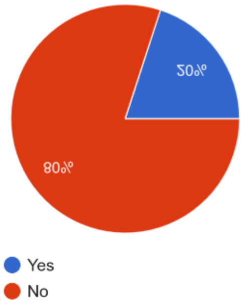
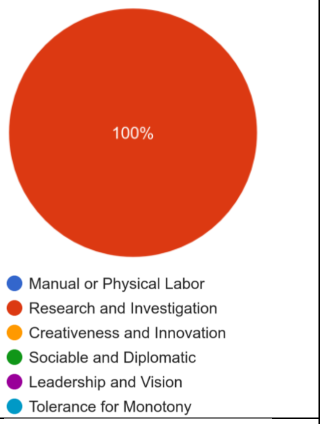
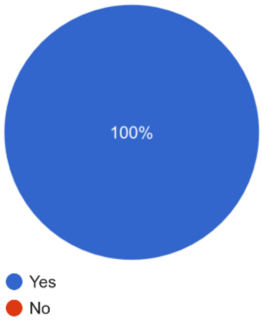
Defensive
- Add "Business" to create "Disaster Recovery and Business Continuity"
- Add "Administration" to create "Security Training Design, Administration, and Delivery"

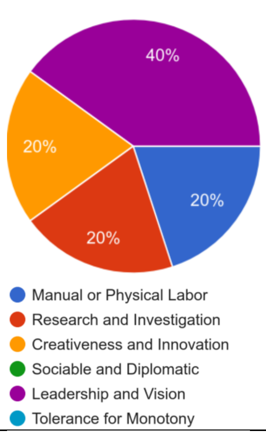
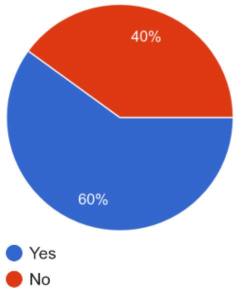
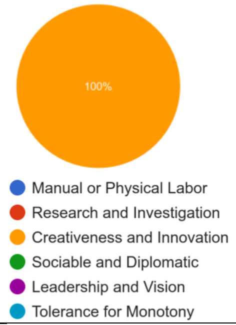
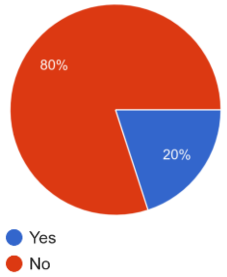
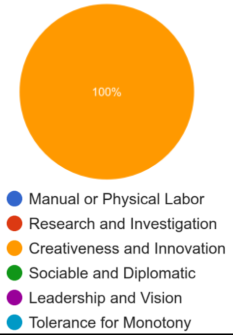
D.4 Cybersecurity Interest-to-Function Survey Data

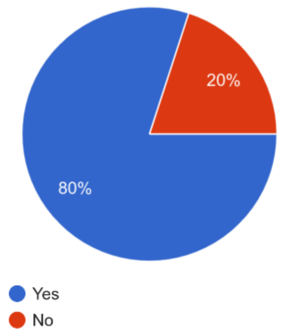
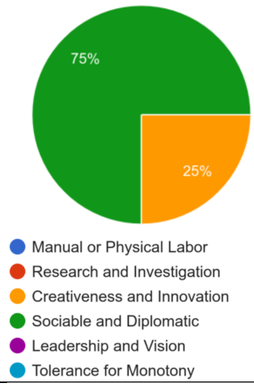
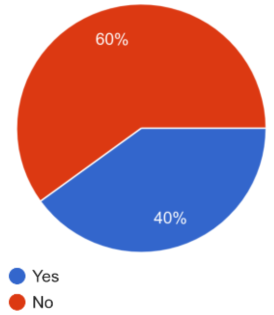
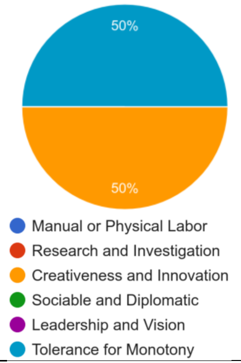
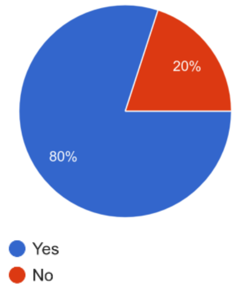
Questions 7 -38

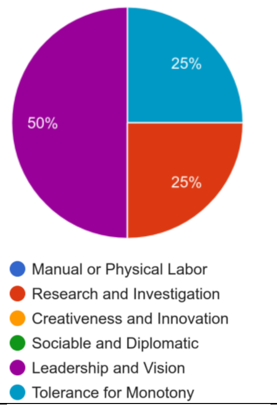
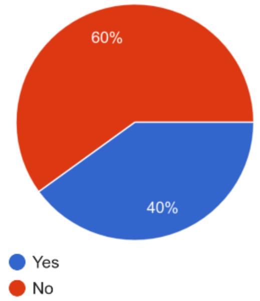
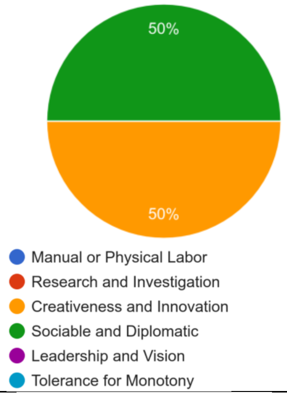
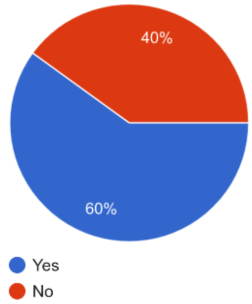
Data Forensics 7. Have you had experience with Data Forensics? *	
Data Forensics - Individual Skills and Abilities 8. In your experience, which individual trait, mindset, or approach is most beneficial when working with data forensics?	
Access Control and Identity Management 9. Have you had experience with Access Control or Identity Management? *	
Access Control and Identity Management - Individual Skills and Abilities 10. In your experience, which individual trait, mindset, or approach is most beneficial when creating access and identity management controls?	
Documentation and Cataloging 11. Have you had experience providing Documentation and Cataloging? *	

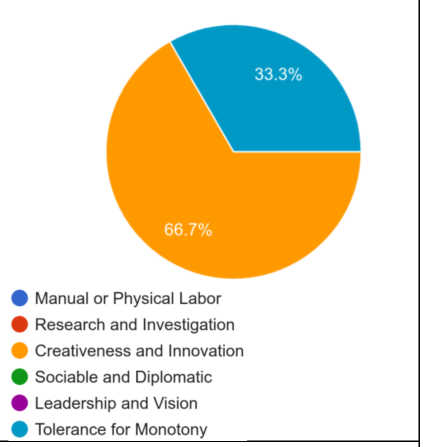
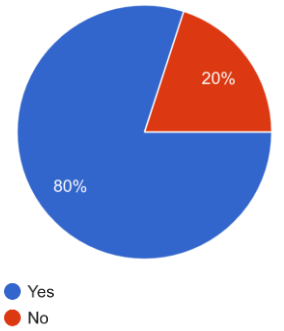
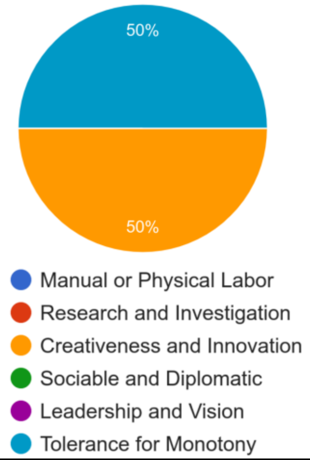
Documentation and Cataloging - Individual Skills and Abilities 12. In your experience, which individual trait, mindset, or approach is most beneficial when documenting and cataloging?	
Physical Security 13. Have you had experience with Physical Security? *	
Physical Security - Individual Skills and Abilities 14. In your experience, which individual trait, mindset, or approach is most beneficial when working with the physical security of an organization?	
Intrusion Analysis 15. Have you had experience with Intrusion Analysis? *	
Intrusion Analysis - Individual Skills and Abilities 16. In your experience, which individual trait, mindset, or approach is most beneficial when analyzing intrusions?	

Legal and Compliance Investigation 17. Have you had experience with Legal and Compliance Investigations? *	
Legal and Compliance Investigation - Individual Skills and Abilities 18. In your experience, which individual trait, mindset, or approach is most beneficial when investigating legal and compliance data for an organization?	
Software Development Security 19. Have you had experience with Software Development Security? *	
Software Development Security - Individual Skills and Abilities 20. In your experience, which individual trait, mindset, or approach is most beneficial when developing software securely?	
Management and Coordination 21. Have you had experience with Management and Coordination? *	

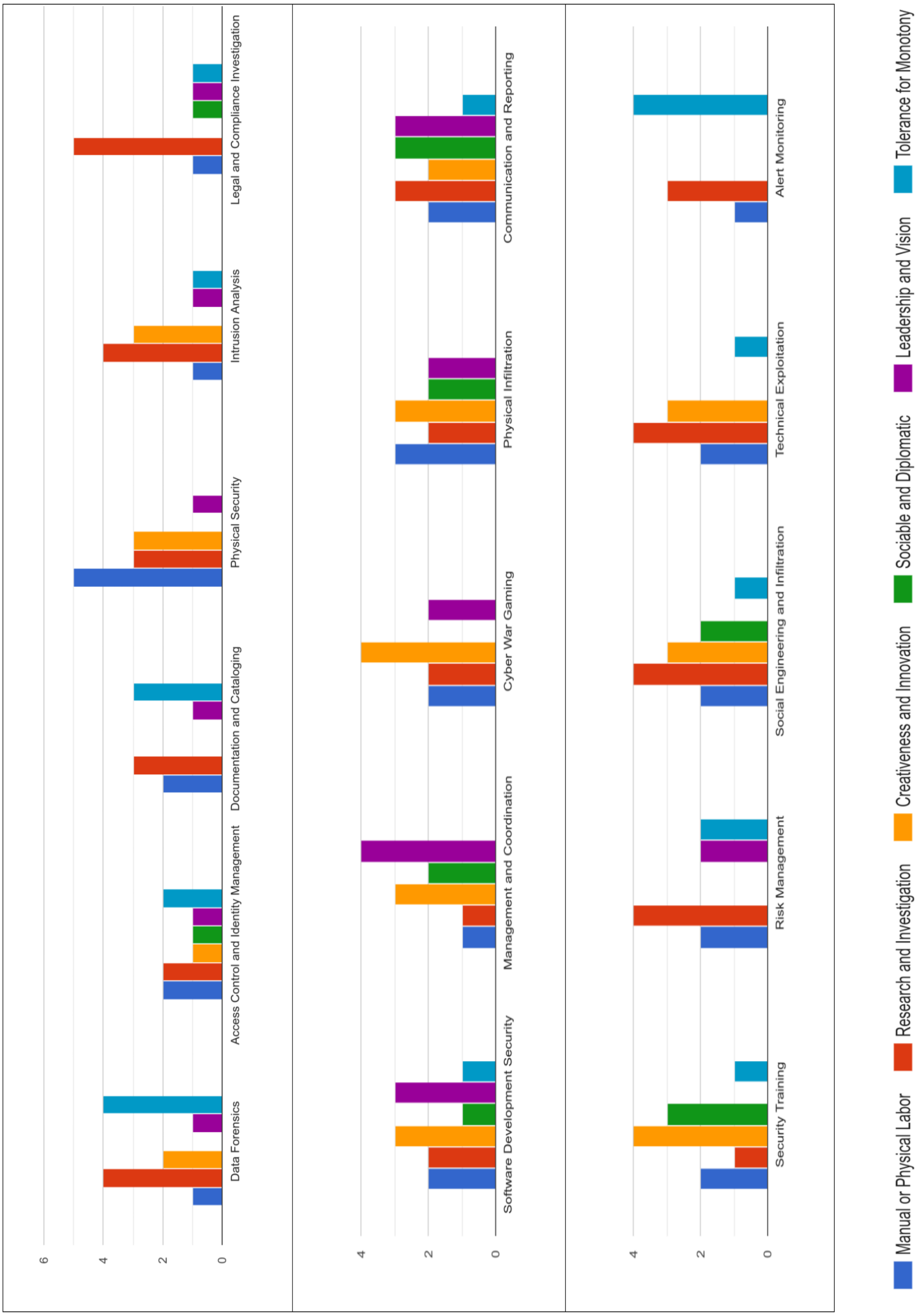
Management and Coordination - Individual Skills and Abilities 22. In your experience, which individual trait, mindset, or approach is most beneficial when managing or coordinating teams at an organization?	
Cyber Wargaming 23. Have you had experience with Cyber Wargaming? *	
Cyber Wargaming - Individual Skills and Abilities 24. In your experience, which individual trait, mindset, or approach is most beneficial when you conducting cyber wargaming?	
Physical Infiltration 25. Have you had experience with Physical Infiltration? *	
Physical Infiltration - Individual Skills and Abilities 26. In your experience, which individual trait, mindset, or approach is most beneficial when physically infiltrating a target site?	

Communication and Reporting 27. Have you had experience with Communication and Reporting? *	
Communication and Reporting - Individual Skills and Abilities 28. In your experience, which individual trait, mindset, or approach is most beneficial when communicating and reporting data within an organization?	
Security Training 29. Have you had experience with instructing Security Training? *	
Security Training - Individual Skills and Abilities 30. In your experience, which individual trait, mindset, or approach is most beneficial when conducting security training?	
Risk Management 31. Have you had experience with Risk Management? *	

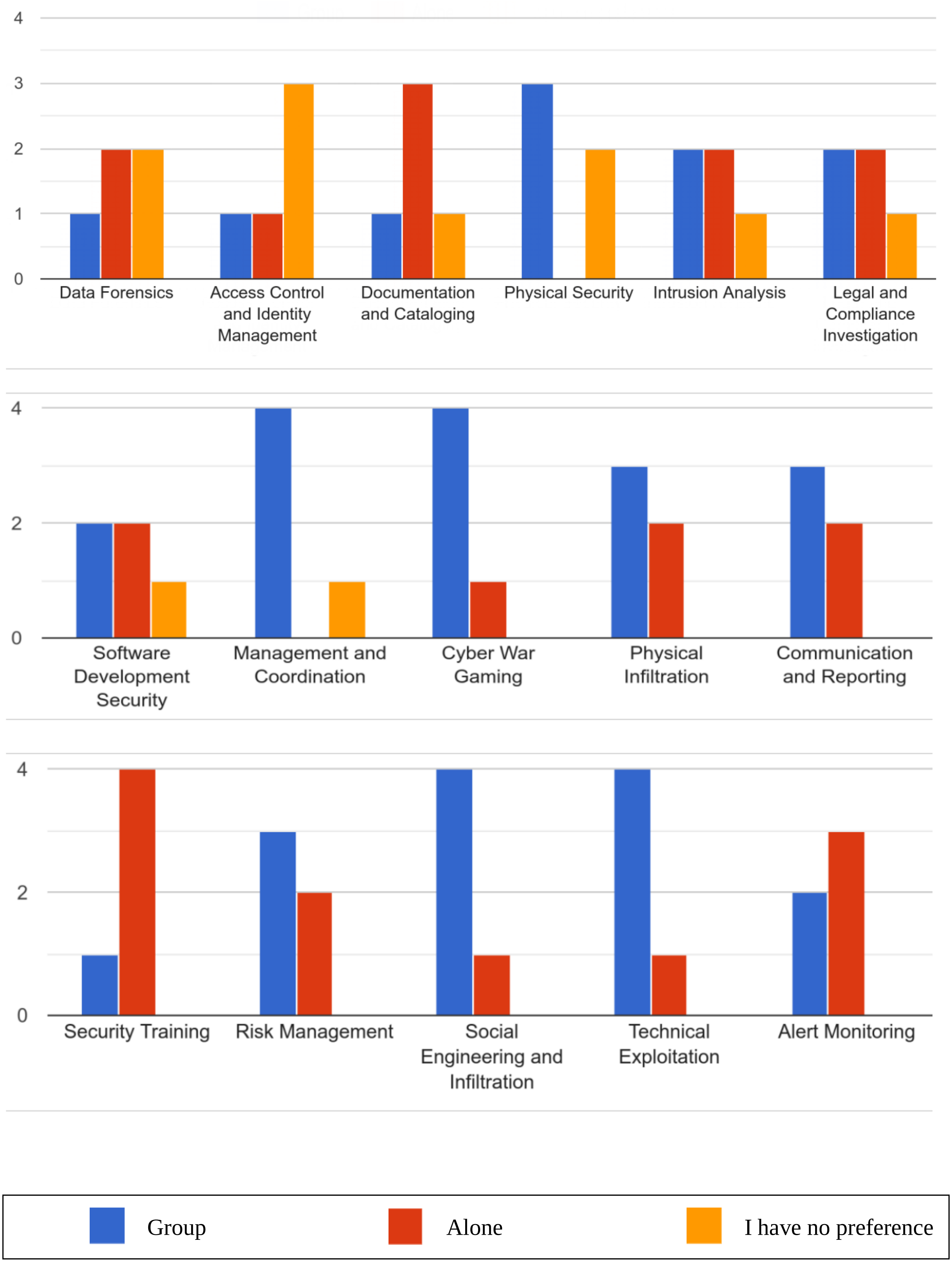
Risk Management - Individual Skills and Abilities 32. In your experience, which individual trait, mindset, or approach is most beneficial when performing risk management functions?	
Social Engineering and Infiltration 33. Have you had experience with Social Engineering and Infiltration? *	
Social Engineering and Infiltration - Individual Skills and Abilities 34. In your experience, which individual trait, mindset, or approach is most beneficial when conducting social engineering and infiltration?	
Technical Exploitation 35. Have you had experience with Technical Exploitation? *	

Technical Exploitation - Individual Skills and Abilities 36. In your experience, which individual trait, mindset, or approach is most beneficial when penetration testing or exploitation?	
Alert Monitoring 37. Have you had experience with Alert Monitoring? *	
Alert Monitoring - Individual Skills and Abilities and Abilities 38. In your experience, which individual trait, mindset, or approach is most beneficial when monitoring the alerts for an organization?	

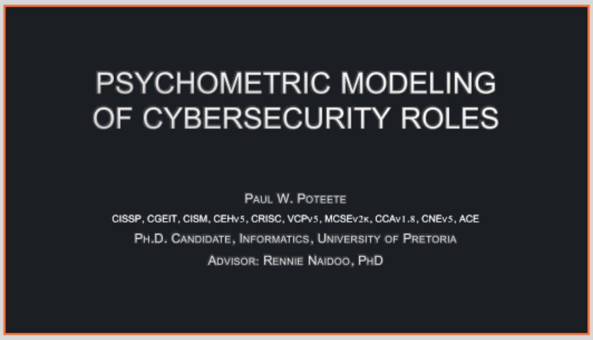
Questions 39-41



Questions 42-44



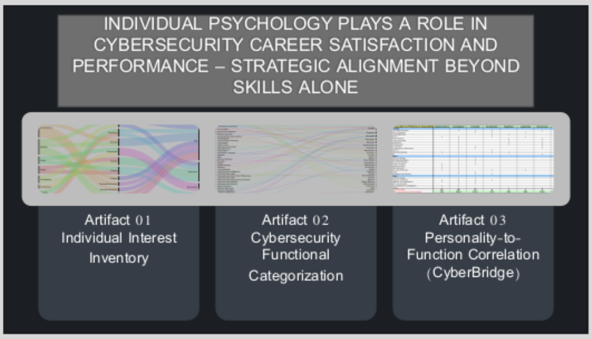
E.1 ICCWS Conference Slides



PSYCHOMETRIC MODELING OF CYBERSECURITY ROLES

Paul W. Poteete
CISSP, CGEIT, CISM, CEHv5, CRISC, VCPv5, MCSEv2k, CCAv1.8, CNEv5, ACE
Ph.D. Candidate, Informatics, University of Pretoria
Advisor: Rennie Naidoo, PhD

1



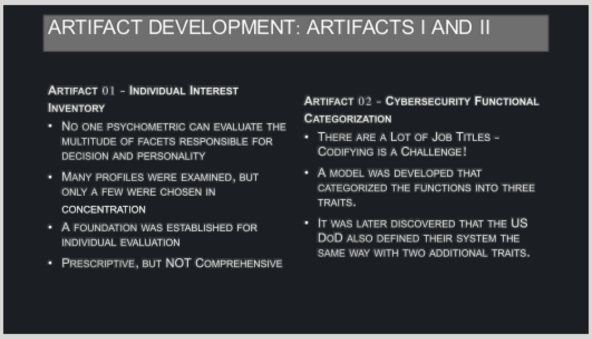
INDIVIDUAL PSYCHOLOGY PLAYS A ROLE IN CYBERSECURITY CAREER SATISFACTION AND PERFORMANCE – STRATEGIC ALIGNMENT BEYOND SKILLS ALONE

Artifact 01
Individual Interest Inventory

Artifact 02
Cybersecurity Functional Categorization

Artifact 03
Personality-to-Function Correlation (CyberBridge)

2



ARTIFACT DEVELOPMENT: ARTIFACTS I AND II

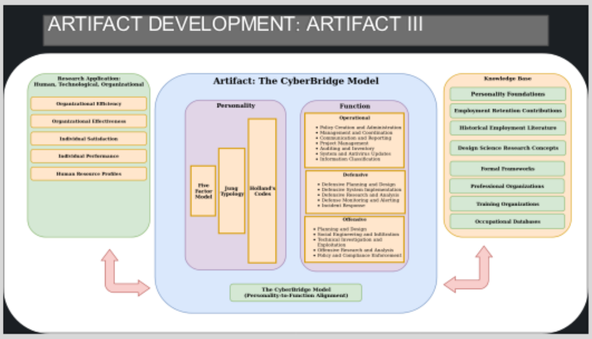
Artifact 01 – Individual Interest Inventory

- No one psychometric can evaluate the multitude of facets responsible for decision and personality
- Many profiles were examined, but only a few were chosen in concentration
- A foundation was established for individual evaluation
- Prescriptive, but NOT Comprehensive

Artifact 02 – Cybersecurity Functional Categorization

- There are a Lot of Job Titles – Codifying is a Challenge!
- A model was developed that categorized the functions into three traits.
- It was later discovered that the US DoD also defined their system the same way with two additional traits.

3



ARTIFACT DEVELOPMENT: ARTIFACT III

Research Application: Human, Technological, Organizational

Organizational Efficiency
Organizational Effectiveness
Individual Satisfaction
Individual Performance
Human Resource Profiles

Artifact: The CyberBridge Model

Personality

Five Factor Model
Jung Typology
Holland's Codes

Function

Operational
- Policy Creation and Administration
- Management and Coordination
- Communication and Reporting
- Project Management
- Auditing and Inventory
- System and Antivirus Updates
- Information Classification

Defensive
- Defensive Planning and Design
- Defensive System Implementation
- Defensive Research and Analysis
- Defense Monitoring and Alerting
- Incident Response

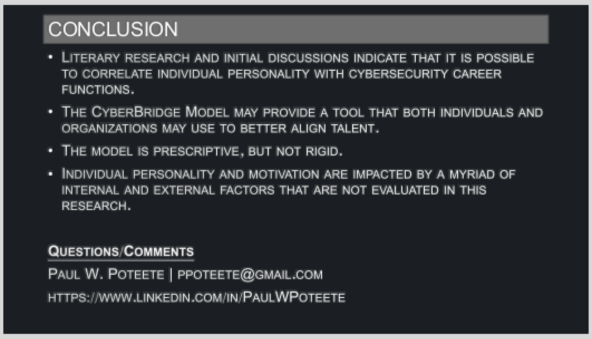
Offensive
- Planning and Design
- Social Engineering and Infiltration
- Technical Investigation and Exploitation
- Offensive Research and Analysis
- Policy and Compliance Enforcement

The CyberBridge Model (Personality-to-Function Alignment)

Knowledge Base

Personality Foundations
Employment Retention Contributions
Historical Employment Literature
Design Science Research Concepts
Formal Frameworks
Professional Organizations
Training Organizations
Occupational Databases

4



CONCLUSION

- Literary research and initial discussions indicate that it is possible to correlate individual personality with cybersecurity career functions.
- The CyberBridge Model may provide a tool that both individuals and organizations may use to better align talent.
- The model is prescriptive, but not rigid.
- Individual personality and motivation are impacted by a myriad of internal and external factors that are not evaluated in this research.

Questions/Comments
Paul W. Poteete | ppoteete@gmail.com
https://www.linkedin.com/in/PaulWPoteete

5

Slide	Content
Slide 1	Psychometric Modeling of Cybersecurity Roles Paul W. Poteete CISSP, CGEIT, CISM, CEHv5, CRISC, VCPv5, MCSEv2k, CCAv1.8, CNEv5, ACE
Slide 2	Individual Psychology Plays a Role in Cybersecurity Career Satisfaction and Performance – Strategic Alignment Beyond Skills Alone Artifact 01 Individual Interest Inventory Artifact 02 Cybersecurity Functional Categorization Artifact 03 Personality-to-Function Correlation (CyberBridge)
Slide 3	Artifact Development: Artifacts I and II Artifact 01 - Individual Interest Inventory No one psychometric can evaluate the multitude of facets responsible for decision and personality Many profiles were examined, but only a few were chosen in concentration A foundation was established for individual evaluation Prescriptive, but NOT Comprehensive Artifact 02 - Cybersecurity Functional Categorization There are a Lot of Job Titles - Codifying is a Challenge! A model was developed that categorized the functions into three traits. It was later discovered that the US DoD also defined their system the same way with two additional traits.
Slide 4	Artifact Development: Artifact III
Slide 5	Conclusion Literary research and initial discussions indicate that it is possible to correlate individual personality with cybersecurity career functions. The CyberBridge Model may provide a tool that both individuals and organizations may use to better align talent. The model is prescriptive, but not rigid. Individual personality and motivation are impacted by a myriad of internal and external factors that are not evaluated in this research. Questions/Comments Paul W. Poteete ppoteete@gmail.com https://www.linkedin.com/in/PaulWPoteete

E.2 ICCWS Best PhD Paper Awarded

Psychometric Modeling of Cybersecurity Roles

Paul Wyatt Poteete
Pretoria University, New Brighton, USA
ppoteete@gmail.com

Abstract: Human psychology plays a role in career satisfaction and performance in every industry. In the face of a global shortage of cybersecurity professionals, and an often difficult team dynamic around these individuals, it is important to define and understand methods of measurement to provide maximum effectiveness and efficiency within an organization. This research analyzes predictors of individual factors of satisfaction and performance for cybersecurity roles through the integration of prominent psychometric analyses. A combination of these psychometric profiles may provide significant predictors for satisfaction and performance in broad categories of cybersecurity roles that are aggregated and condensed from NIST and several other sources. This research could provide organizations with tools to increase both agility and performance within cybersecurity functions and teams. The work is being conducted through the design science research methodology (DSRM). This allows for the creation of artifacts that address the use of psychometric measurements as predictors for individual psychological factors in cybersecurity roles. Organizations are faced with non-traditional, asymmetric threats from a myriad of cyber-connected sources. A positive conclusion would result in organizational predictors for cybersecurity functions, as well as, opportunities for organizational realignment to allow for unique psychological traits in non-traditional business operations. The findings will contain the created artifacts and results of surveys of cybersecurity professionals. The artifacts will reveal the correlation between the integrated psychometric profiles and cybersecurity functions, exposing their potential to be used as predictors for increased organizational efficiency and effectiveness as reflected by individual satisfaction.

Keywords: Cybersecurity, Role, Psychometric, Performance, Satisfaction

1.Introduction

1.1Cybersecurity global shortage

There is a global shortage of skilled cybersecurity staff facing organizations of every kind and location. The proper selection of a skilled and culturally competent employee is critical to the security and productivity of the organization. Recently, in “The Cybersecurity Workforce Gap,” it is stated that "By 2022, the global cybersecurity workforce shortage has been projected to reach upwards of 1.8 million unfilled positions" (Crumpler & Lewis, 2019). “This global shortage is also faced with predictions that the shortage will not soon be improving” (Oltsik, 2017). This research proposes that a work environment that aligns with individual personality preferences is paramount to organizational success.

This research maintains that the shortages are facilitated by more than economic and cultural factors; they are also influenced by inefficiencies created through the misalignment of individual psychology to cybersecurity functions. As job functions are properly aligned with the respective individual personality types, capable staff will continuously fill a greater number of positions. The proper integration of functional requirements aligned to the individual's personality profile will aid in the career satisfaction enjoyed by each member. This improvement may have a measurable effect on the number of skilled security candidates available at an international, national, and local level for organizations and governmental offices. Offices benefiting from this alignment may additionally be awarded with greater employee retention as well as organizational performance and individual morale.

The purpose of this study is to establish an association of psychological traits to career functions for the cybersecurity workforce, in such a way, as to allow the creation of a formulaic solution for both career-seekers as well as employers that predicts individual job satisfaction and performance. Through this process, it is expected that a new artifact will be generated that is called, "The CyberBridge Model" that will more closely define personality factors to cybersecurity functions. The CyberBridge artifact (see Figure 2) is described in more detail in Section 4: Conceptual model and artifact development. Through the creation of a better suited model of "cybersecurity function" to "personality factor," it is hoped that individual satisfaction and organizational performance can be improved.

2.Background and literature review

2.1Cybersecurity challenges

The challenges surrounding cybersecurity functional, psychological, and organizational alignment go beyond human resource shortages. It may be seen as extending into a type of asymmetric battlefield operation that is conducted invisibly alongside normative organizational processes. The difficulty of implementing cybersecurity programs may be seen as a combination of the lack of understanding of cybersecurity functions, the proper individual psychological alignment with those functions, and how those functions may be communicated in business terminology. In many cases, cybersecurity operations may be seen as more similar to that of a battlefield than a business. Organizational operations, including technical operations, can be measured against well-established productivity models. This may be contrasted with cybersecurity threat models that are being actively developed in such radical ways that organizational policies, standards, and procedures may not be able to maintain the magnitude of changes that occur from one day to the next (Mikolic-Torreira et al., 2017). The proper identification of cybersecurity functions, and the integration of appropriate personnel, will aid in the prevention, detection, and remediation of more than the common attacks, it is expected to provide a solution for the advanced persistent threats that deliver serious challenges to current program models. A properly aligned team, organized into skilled operational, defensive, and offensive staff, working in concert with autonomous systems, contend against the onslaught of attacks that confront organizations today and in the future.

2.2Cybersecurity in perspective

The involvement of diverse categories of human psychology, and its impact on cybersecurity programs, may not be immediately clear in some instances. To better understand this relationship, a short background of how its developmental history is framed within this research could be of assistance. The immediate origins of cybersecurity come from the early concepts of computer and information security. The original term that is mostly closely aligned to today's information security would be the expansion of computer security from the 1960s. Computer security became commonly referenced as information security in the 1970s and beyond (Lin et al., 2012). This maturation of this new industry could be seen as the realization emerged that it was not the actual "computer" that needed protection, but it was indisputably the information contained therein (Greene, 2014). In this age, as computer systems, networks, and applications are becoming more complex, the term cybersecurity is more appropriate in many instances. This is because cybersecurity and information security relate with two different abstract concepts. This differentiation may be expressed in the conceptualization that the term, "information security" represents the protection of near tangible resources, and the term, "cybersecurity" represents an intangible symbiotic orchestration of protective processes. This may be more clearly communicated in that the concept of cybersecurity is the combination of both autonomous system processes and manual human input. This synergistic combination is most closely identified through its origins in the term, "cybernetics" that was coined by Norbert Wiener in the late 1940s, in which he noted the concept of machine-human interaction (Wiener, 1961). In regard to this differentiation, the term, "cybersecurity" represents more than computer or information security, it represents the orchestration of autonomous systems working in concert with human intelligence to produce output greater than the sum of its parts. Through understanding that cybersecurity systems are not in exclusion to human influence, but operate as a result of human influence, individual psychology can be seen to play a larger role in cybersecurity operations and organizational performance.

3.Cybersecurity functions and categories

Cybersecurity roles may be largely misunderstood within industries as a result of the immaturity, novelty, and complexity of their functions. The challenge of defining the complex functions within these roles is exacerbated by the uniqueness of the new capabilities and threats. As many of these roles have existed for less than a decade, only active individuals within the respective industries and functions are capable of providing insight into their actual function. The operational functions are better defined and understood, as they have been conducted over several decades, especially since the advent of large-scale use of computerized resources from the 1970s. This creates a rapid pace of development of not only new technologies and their associated risks, but of employee functions within the support and design roles surrounding those technologies (DeSilver, 2014).

3.1Formal frameworks

Cybersecurity frameworks provide organizations with structural and procedural support for organizations to assist in the development of cybersecurity strategies, usually with a limited attempt to define cybersecurity roles. These explanations are often ambiguous or contradictory, as in the definition of a cybersecurity analyst, or conversely, they may have reached considerable consensus, as in the description of the duties of a Chief Information Security Officer (CISO). Although the function and tasks associated with each respective cybersecurity role may be a small portion of the framework, the ultimate goal of the framework allows deduction into what individual responsibilities may be relevant. In some instances, frameworks establish educational recommendations for cybersecurity functions without listing specific role designations. This allows an organization to address the most fundamental needs of the program without the complications found in politicized role titles (Newhouse et al, 2017). In any case, an organization should strive to align the framework with their regulatory and industrial needs as well as their cultural foundations. The two frameworks discussed in this portion of the research are the National Institute for Standards and Technology (NIST), National Initiative for Cybersecurity Education (NICE), and the International Organization for Standardization (ISO). Although this is not a comprehensive list, it does provide a dichotomous expression of interests (ISO/IEC, 2014; Newhouse et al., 2017).

3.2Professional organizations

Professional organizations possess substantial influence in the training and promulgation of an assorted collection of cybersecurity careers. One such certification, the Certified Information Systems Security Professional (CISSP®), provided by the International Information Systems Security Certification Consortium (ISC)² is internationally respected as the most significant certification for senior cybersecurity professionals ((ISC)^2, 2018). This certification is currently accepted within many national governments as proof of knowledge in part of their cybersecurity professional requirements. Next, the Information Systems Audit and Control Association (ISACA), has international distinction for their certifications, the Certified Information Systems Auditor (CISA®) and the Certified Information Security Manager (CISM®) (ISACA, 2018). Although almost every professional organization has several certifications, (ISC)² and ISACA® are highly-regarded within the security industry as providing authoritative training and education.

3.3Training organizations

Due to the complexity involved in the leadership, design, administration, and auditing of cybersecurity functions, several organizations have arisen to meet the challenge of training individuals interested in cybersecurity for their future roles. Two representative institutions are: the SysAdmin, Audit, Network and Security (SANS) Institute, and the InfoSec Institute. These organizations provide specific training for tasks encountered in everyday work by cybersecurity professionals. SANS is possibly the largest provider of cybersecurity training in the world (SANS Institute, n.d.). The InfoSec Institute is a newer organization that gained popularity through the introduction of an ethical hacking certification. As InfoSec Institute has grown, it has become internationally recognized for its hands-on, practical training (Institute, 2018). Both of these organizations represent a multitude of training organizations that are now dedicated to cybersecurity career training. As training becomes more refined, the clarity of each cybersecurity function becomes more defined. The increasing levels of clarity surrounding each position allow this research to more accurately align psychometric profiles to cybersecurity roles and career outcomes.

3.4Occupational databases

Finally, occupational databases that contain job statistics and functional definitions of vocational tasks provide the ability to target personality-to-function metrics for cybersecurity career retention. The Occupational Information Network (O*NET) Program provides validated data for the entire United States workforce, which is freely available for scientific or personal research purposes (U.S. Department of Labor, n.d.). The incorporation of Holland's Codes (RIASEC) evaluations into the career database also provides insight into personality-to-function directly for many careers. This allows for extensive data to be drawn for general careers that may then be related to cybersecurity career performance and retention.

3.5The Importance of individual psychology

Psychometric profiling helps subdivide personalities into discrete segments, allowing the application of personal traits to potential outcomes. There are a seemingly unlimited number of profiles available; however, this research has focused on psychometric evaluations that appropriately cover the range from broad to specific traits that would be helpful in determining job retention or satisfaction in a cybersecurity career discipline. Additional research was required to determine the caveats of psychometric testing to properly determine how the test results would relate to a particular trait, condition, or situation of employment. This led to research into the congruity between psychometric examinations that provided both links to other profiles and complimentary theories surrounding individual psychology. These additional references created the need for methods by which they may be analyzed more clearly. To attain additional clarity, categories were developed to better define what psychometric profiles are used as a representative foundation. The categorization provides this research with a focused definition of each category of psychometric models and correlation in a succinct manner through the use of representative texts relating to each of the developed categories.

3.6Psychometric delineation and integration

Included in the complexities of defining cybersecurity functions and staffing shortages, the proper alignment of personality traits to cybersecurity positions has an impact on more than the individual's well-being; it influences the overall organizational security and profitability. If consideration is taken to determine how well an individual may work in a complex security role, actions can be taken to maximize employee satisfaction and minimize organizational loss. It may be possible to produce these outcomes through an increased understanding of cybersecurity functions and individual psychological tendencies. Understanding both the organization's specific needs and the individual's personality traits is critical to improving cybersecurity employee retention and organizational productivity.

The alignment of personality traits to cybersecurity positions is complicated by two primary factors: 1) employee personality traits are not analyzed for cybersecurity role performance or satisfaction objectives and 2) cybersecurity functions are often poorly defined, leaving a lack of clarity to the operational definitions of the role. These issues are compounded by the complex nature of public and private organizational security requirements and the difficulty in adequate measurements regarding human personality factors.

Several psychometric evaluations were considered for use in this research. The predominant solutions identified for employee evaluations were the Five Factor Model (FFM), DISC®, MOTIV, Ennegram, Jung/MBTI®, and the Holland Code (RIASEC). Of these, the FFM, Jung/MBTI®, and RIASEC are the evaluations considered effective for correlating personality type with cybersecurity job function as relevant to this research. Each psychometric profile offers insight into a multitude of individual preferences. This research presents that the following aspects of each psychometric are significant in the determination of alignment for cybersecurity functions, as limited by the respective psychological profile's ability to determine this level of specificity. The following section contains a short description of each profile as interpreted for this research.

The Big Five personality traits test, or the Five Factor Model (FFM), often known as the "Big 5," summarizes personality traits using a lexicon of adjectives, and groups personality types into five factors of openness, conscientiousness, extroversion, agreeableness, and nueroticism (Digman, 1990).

The Jung Typology represented personality in eight distinct modes (Jung, 1921). This research was augmented by Myers-Briggs to include additional traits that extended the Jungian Typology to a total of sixteen individual traits (Myers, 1998). This is both representative of the Extended Jungian Typology and Myers-Briggs Type Indicator® (MBTI®). This involves combinations of introversion/extroversion, intuition/sensing, feeling/thinking, and perceiving/judging (Jung, 1921).

John Lewis Holland, an American psychologist, has profoundly influenced vocational psychology by developing and creating the career development model called the Holland Occupational Themes. This typology, which is also called the Holland Codes or RIASEC, is unique because it simplified the process of psychometric testing and has directed countless individuals to a career. The Holland Codes are composed of tasks that considered: realistic, investigative, artistic, social, enterprising, and conventional (Holland, 1986).

3.7Design Science Research Methodology (DSRM)

DSRM provides an appropriate foundation for the development of new artifacts within the information systems (IS) community, especially since the IS field is involved with the use and development of new technologies and paradigms (Peffers, Tuunanen, & Niehaves, 2018). The recent trend shows that information systems researchers have gravitated towards DSRM in recent years, especially those with a vision and a desire to make a global impact with their knowledge (Thuan, Drechsler, & Antunes, 2018). This integration of information system expertise and vision allows researchers the ability to promote and investigate their designs in a measured and consistent manner. This is reinforced by the increased popularity of design science research (DSR) within the information systems field that has occurred over the years through a plethora of DSR publications at conferences and within research articles surrounding information systems publications (Deng, Wang, & Ji, 2017; Hevner & Chatterjee, 2010; Peffers et al., 2018). DSRM provides a framework that lends itself to novel artifact development that is useful when designing new approaches to cybersecurity, as cybersecurity defensive and offensive controls often follow an unusual path when solving problems. DSRM is also useful in the punctual creation of new capabilities through artifacts that could be used to address the myriad of cybersecurity-centric challenges that arise moment by moment.

4.Conceptual model and artifact development

This research falls within DSRM, allowing for the development of solutions to meet challenges in creative endeavors. Primarily represented by Figure 1 below, the process involves an adaptation of the following: Problem Identification, Proposal, Design of Artifacts, Initial Publication, Evaluation, Revision, Conclusion, and Final Publication of the solution (Vaishnavi et al., 2017, p. 8). This may vary in some ways to methodologies that allow for negative or null conclusions that do not provide a final solution to the original challenge. DSRM allows for multiple iterations to be re-crafted to address areas where the challenge was unsolved, allowing the researcher to continue to refine their solution to meet new or factors that were not properly defined.

Figure 1: Design Science Research Methodology (DSRM) (Vaishnavi et al., 2017, p. 8)

This research is centered on several traits have been identified which are believed to explain the association of individual employee personality traits to cybersecurity job functions. It is believed that these traits may be empirically measured to produce meaningful statistical representations of employee satisfaction and efficiency. There are several job retention models that offer solutions based on organizational input into the employee's work experience as an explanation of retention intention, as well as, some models that offer personality trait correlation to broad industry. This model will examine individual employee personality traits in direct relation to the individual's tasks within the scope of cybersecurity functions as indicators of satisfaction, performance, and possibly, retention. It is believed that this alignment will influence an employee's satisfaction and performance within cybersecurity roles. To accomplish this task, this research will create three artifacts. The first is related to psychometric integration, the second is a new categorization of cybersecurity functions, and the final artifact is a correlation of the first two artifacts that is labeled, "The CyberBridge Model (see Figure 2)."

Figure 2: The cyberbridge model

4.1Artifact 01 - Psychometric delineation and integration

Through this research it became apparent that a single psychometric profile would not be sufficient to address both the functional requirements for correlation to cybersecurity careers and individual personality factors. Several models were created to correlate the various psychometrics and cybersecurity functions into a single cohesive model for causality; however, it was determined that each of the psychometrics analyzed a different aspect of performance and satisfaction, preventing the understandable usage of a causal model spanning each of the factors expressed in a single psychometric. Eventually several psychometric profiles were grouped to achieve a single goal. To correlate these performance and satisfaction outcomes with cybersecurity functions, discrete metrics are used to represent individual psychological traits. The specific psychometrics used for this study are The Five Factor Model, Jung Typology, and Holland's Codes. Preexisting and well-established psychometric evaluations were selected due to their history of successful research application and human psychological relevance (Tokar, Vaux, & Swanson, 1995). This avoided the creation of an entirely new psychometric that would require extension analysis prior to its usage in modeling individual outcomes and predictions.

To accomplish the logical integration of the three psychometric profiles, it was first necessary to delineate the traits defined within each profile. The Five Factor Model, Jung Typology, and Holland's Codes were individually indexed, then aligned to remove any duplication of measurements from each profile, then reintegrated into a single tuple of psychological measurements. This created a relation instance that could be associated with each cybersecurity function attribute defined into a matrix. This matrix can then be used to assign a binary indicator to each attribute value as it applies to both the psychometric tuple and functional attribute. This is visually represented in Figure 3 below.

4.2Artifact 02 - Cybersecurity functional categorization

There are thousands of current cybersecurity titles and related job descriptions reported online (Zeltser & Hoyt, 2015). The complexity of the cybersecurity field is similar to what is seen in the healthcare industry, but far fewer people are familiar with cybersecurity functional distinctions. Cybersecurity functional identification is further complicated by the plethora of Cybersecurity job titles that are utilized to describe similar or identical information security roles in an organization. In order to organize these roles into workable categories that align to individual personalities, a categorization should be created. This research establishes a fundamental set of cybersecurity functions within three broad categories that will allow for their correlation to psychometric results. The three general categories are: Operational, Defensive, and Offensive tasks.

To index and codify these categories, a compiled list of over 3,000 cybersecurity job titles was created from 1) formal frameworks: NIST/NICE and the ISO 27000 series, 2) professional organizations: (ISC)² and ISACA, 3) training organizations: the SANS Institute and InfoSec Institute, and finally, 4) the occupational databases from the O*NET Program. This provided several data sets that have proven validity for the cybersecurity industry. After aggregating the list, normalization was initially conducted through common tools such as, cat, sort, uniq, grep, and awk, with additional codification through Gnumeric's table and descriptive functions. In the final stage, each of the functional job titles were broken down into common daily tasks as they related to cybersecurity. These tasks were grouped into the three aforementioned categories of Operational, Defensive, and Offensive tasks. In order to maintain the cybersecurity focus of this research, functions such as cryptography and secure programming were defined only as security functions when they directly applied to security controls. This excludes cryptography when viewed as purely mathematical and secure programming when seen as strictly a programming methodology without regard to the software's intended use. An example of the final categorization is listed below.

Operational Functions
- Policy Creation and Administration
- Management and Coordination
- Communication and Reporting
- Auditing and Inventory
- System and Antivirus Updates
- Information Classification

Defensive Functions
- Defensive Planning and Design
- Defensive System Implementation
- Defensive Research and Analysis
- Defense Monitoring and Alerting
- Incident Response

Offensive Functions
- Offensive Planning and Design
- Social Engineering and Infiltration
- Technical Investigation and Exploitation
- Offensive Research and Analysis
- Policy and Compliance Enforcement

4.3Artifact 03 - Correlation of psychometric results to cybersecurity categories

The final artifact is titled, "CyberBridge," as it correlates the psychological and functional cybersecurity aspects into a single prescriptive model. This model is initially created through common association of cybersecurity functions to known personality markers. As this is the seminal work in this area, additional research would involve surveys and focus groups to validate the correlation.
Figure 3: Psychological and functional correlation example for the Holland's Codes

The focus group interviews are open format with guided questions to maintain relevance. An example is provided below.

Part I - Basic Demographics
What is your position within your organization?
What level of experience do you possess?

Part II - Open-ended free-form discussion about Personality and Function
What are the most common cybersecurity tasks with which you are involved on a regular basis?
What personal traits do you feel help you the most in coping with that particular challenge?
This process is repeated for every functional task discussed by the subject.

Part III - Structured Opinion

Based on the three categorizations (listed below), what omissions or changes would you feel are appropriate?

The survey is open to all individuals who are serving, or have served, in a cybersecurity functional role. Titles are excluded, as they were found to be not representative of the functional work performed by each individual. The survey measures which functions are identified by the respondent, their satisfaction with the specified function, and their results for the Five Factor Model, Jung Typology, and Holland's Codes.

5.Results and discussion

Research will be conducted by surveys, using psychometric profiling solutions and a short questionnaire. This will be conducted almost entirely online through direct email, social media, blogs, and automated mailing systems to the target population. Some data may be collected via in-person interviews; however, this is expected to be a minor portion in the initial phase of collection. The data collected will be quantitatively compared to the null hypothesis of this research to provide insight into the individual's job satisfaction and desire to maintain employment in their position as related to specific cybersecurity functions.

At the time of this writing, results are based on literary source materials. The literary sources seem to agree with the influence of individual psychology on job performance (Biggio & Cortese, 2013). Targeted investigation within cybersecurity career-holders through individual focus groups and large-scale surveys should be conducted to allow for a diversity of data sets, as well as, targeted data collection specific to this model development within cybersecurity employees for validation.

This research supports that a model can be successfully developed to better align cybersecurity functions with individual personalities. This is possible because individual experiences are relative to an individual's psychology, which can be appreciably quantified through psychometric testing. The delineation of cybersecurity functions for individual satisfaction is supported, as one's personal interpretation of any particular experience is relative to their own individual psychology. Individual psychology may be profiled, to an extent, through psychometric analyses. These psychometric analyses, albeit limited, may provide measurements that can be quantified into each individual relative experiences. These quantifiable psychological traits may then be associated with experiences encountered while engaged in specific job functions, insomuch, as these functions can be grouped/categorized/classified into general, routine or frequent categories. The resulting quantification of individual psychological traits may be aligned with the functional categories to provide a model/table of personality-to-function recommendations that would both improve individual satisfaction as well as organizational performance.

6.Conclusion

The cybersecurity industry, and the functions therein, are diverse. As is similar in industries concerning aeronautics or healthcare, a single personality type would not be sufficient to account for the myriad of functions presented in each role. This requires the careful delineation of cybersecurity functions and their correlation to psychometric profiles to provide individual results. The shortage of cybersecurity candidates, combined with potentially misaligned cybersecurity programs, creates an environment where increased accuracy for psychometric alignment to requisite cybersecurity functions is recommended.