



Part 2

6 A Digital Forensic Readiness Framework for Information Privacy Incidents

6.1 Introduction

In Chapter 2 we defined information privacy as “the right of individuals to control, or at least significantly influence, the acquisition, access, use, dissemination and veracity of information about themselves” (Clark 2006). We also discussed how the protection of information privacy is mandated by law in many countries. Organisations operating in such countries therefore have a legal obligation to protect the information privacy of data subjects. Over and above the legal obligations that may exist in certain countries, both consumers (Jordaan 2003) and ethical corporate governance standards (Lau 2001) demand that information privacy is protected, regardless of an organisation’s geographic location.

Digital forensic readiness (DFR), on the other hand, was defined in Chapter 4 as “those actions, technical and non-technical, that maximize an organisation’s ability to use digital evidence whilst minimizing the costs of an investigation” (Rowlingson 2004, p.5). An organisation’s DFR capability requires carefully considered and coordinated participation by individuals and departments throughout the organisation (Rowlingson 2004, p.21) in order to be most effective. In other words, a DFR capability that is developed or executed in an ad-hoc manner is not as likely to succeed (Endicott-Popovsky et al. 2007, p.8).

The concepts of information privacy and DFR intersect when a violation of information privacy occurs and it is necessary, or preferable, to conduct a digital forensic investigation into the violation. A violation of information privacy can be security-related, that is, it can result from a breach of an information security control. For example, a breach of access control may result in unauthorised access to private information (PI). An information privacy violation may be more complicated – it may result from inappropriate use of PI by individuals duly authorised to access it. Likewise, privacy laws may also require a response to privacy violations that go beyond apprehending the perpetrator and closing security loopholes – for instance, there may be a

A Digital Forensic Readiness Framework for Information Privacy Incidents

legal requirement to notify the affected data subjects of the privacy breach (Hutchins et al. 2007). Therefore, organisations with a DFR capability designed to deal with security-related incidents may not be in an optimal position to respond to and investigate privacy-related incidents. To address this issue, we propose a framework that considers the additional requirements for organisations for ensuring DFR with respect to information privacy incidents. The term ‘framework’ however, is used widely in the literature with various meanings. We use the following definition for the term as it relates to the framework presented here:

A collection of the organisational policies, business processes, practices, functions and structures, as well technologies that are needed to meet an organisational objective. The collection is organised in such a way that the inter-relationship between the elements contained in the collection is described.

For this thesis we use the definition of a business process given by Hammer and Champy, which was cited in Lindsay et al. (2003), namely: a set of partially ordered activities intended to reach a goal. In the framework presented here, the organisational goal is to ensure that DFR for information privacy incidents is adequately dealt with.

In keeping with the definition of a PET and the classification of PETs in Section 2.3.5, the framework can be considered a HLO PET. It should be noted, though, that the framework is also meant to be used in large organisations with a mature information security function. Mouhtaropoulos et al. (2011, p.193) note that a mature information security function is critical for a DFR programme to be successful. Moreover, information security is necessary in order to protect information privacy.

Our framework is intended to be an ideal, or theoretical, representation of a generic digital forensic readiness capability for dealing with information privacy violations within large organisations. The terms ‘ideal’ and ‘theoretical’ indicate that the framework is not subject to cost or other organisational constraints. The framework aims to provide a basis upon which organisations can build a digital forensic readiness capability for information privacy incidents (FORCFIPI). Since DFR requires participation from individuals at all levels and across departmental boundaries, the

A Digital Forensic Readiness Framework for Information Privacy Incidents

purpose of the framework is to provide guidance at a high level by showing the policies, business processes and organisational functions that are necessary for DFR. It also allows an organisation to determine the low-level, or device-level digital forensic procedures, standards and processes required to implement a digital FORCFIPI.

In this thesis we limit the scope of our work to the structural aspects of the framework rather than the procedural aspects. The term ‘structural aspects’ refers to the choice of the elements contained in the framework as well as the relationship between each element. The ‘procedural aspects’ of the framework consist of the practical measures necessary to implement such a framework in an organisation. Detailed procedural aspects are not included in the scope of this work for two reasons: 1) they are primarily the subject of the academic field of Organisational Behaviour and Management (Ivancevich & Konopaske, 2010); and 2) we believe that the research required on how best to implement a digital FORCFIPI is too large to include within the scope of this work. A brief discussion on how the framework can be implemented is provided, albeit at a high level, for the sake of completeness.

It is critical that the structure is correct before proceeding to the procedural aspects. This is in order to avoid implementation problems that are a result of incorrect design decisions in the structure of the framework. The structural aspects of the framework are, however, still a significant contribution to the treatment of information privacy in the forensic readiness literature, since, to our knowledge, no prior work on this topic has been published besides our own (Reddy & Venter 2009). In fact, even without considering information privacy, the only comprehensive framework for digital forensic readiness (DFR) applicable at the organisational level is the work by Endicott-Popovsky et al. (2007) mentioned in Chapter 4. Barske et al (2010) propose a DFR framework for small to medium size South African enterprises, however, it is not comprehensive in comparison to Endicott-Popovsky et al. and Reddy & Venter (2009). It also focuses on small to medium size organisations rather than large organisations, which are the subject of this thesis.

When considering privacy, though, the vast majority of work deals with the privacy of computer users against forensic analysis – so-called ‘anti-forensics’. Examples include

A Digital Forensic Readiness Framework for Information Privacy Incidents

work by Caloyannides (2004), Antoniou et al. (2008), and Berghel (2008). In a review of the literature we did not find any work, other than our own, dedicated to the use of DFR as a means of ensuring the twin aims of protecting data-subjects' information privacy, and ensuring organisational compliance with information privacy laws. Moreover, we did not find any comprehensive treatment of information privacy in the DFR literature.

This chapter is structured as follows: Section 6.2, which follows, explains why information privacy incidents require a different approach to DFR than the traditional approach for security-related incidents. Section 6.3 presents our framework and in Section 6.4 we present a high-level discussion on how it may be implemented in an organisation. We conclude the chapter in Section 6.5.

Much of the contents of this chapter have been published in edited form in the proceedings of the IFIP 11.9 Conference on Digital Forensics (Reddy & Venter 2009).

6.2 Rationale for a privacy-specific approach to forensic readiness

In this section we explain why a digital forensic readiness capability for information privacy incidents (FORCFIPI) requires a different approach than the traditional approach followed for security incidents.

In an organisation that has mature information security practices, information security controls are typically in place to mitigate risks (Stacey 1996)(IT Governance Institute 2005, p.177). If information security controls fail, this may result in an incident, which often forms the subject of a DF investigation. Traditionally, information security is concerned with the confidentiality, integrity and availability (CIA) of information (Taylor et al. 2007, p.101). Information privacy, on the other hand, is concerned with the ethical or legal use of information rather than the CIA thereof (Burkert 1998, p.125). CIA is, however, a necessary, albeit, insufficient condition for information privacy (Burkert 1998, p.125). This implies a wider range of potential violations or incidents since the ethical or legal usage requirements are in addition to the traditional requirements for security. This also implies that additional controls and DFR measures are needed to prevent and investigate the increased number of potential violations and incidents. A

A Digital Forensic Readiness Framework for Information Privacy Incidents

digital FORCFIPI provides guidance with regard to these additional controls and DFR measures.

Further to the additional controls and DFR measures, the ethical or legal usage requirements necessary for information privacy directly affect the business processes of an organisation. This is because privacy-related business processes³ form a significant part of how an organisation uses information. Changes to existing business processes may be necessary, or new business processes may be required. In order to determine the necessary changes, the acceptable use of data subjects' information needs to be defined. Ideally, acceptable use boundaries for business processes are specified through policies (Taylor et al. 2007). In order to specify the limits of acceptable use, policies should be derived from authoritative sources such as information privacy laws and/or ethical guidelines. Hence, in an organisation, policies are the primary source of guidance to ensure that business processes (including DF processes) adhere to the appropriate ethical or legal usage requirements. As mentioned, in some instances ethical guidelines, such as the Fair Information Principles (FIPs) mentioned in Chapter 2, may necessitate entirely new business processes that deal specifically with private information – we term these new business processes, privacy-specific business processes. A digital FORCFIPI is based on policy and contains the FIPs and privacy-specific business processes, all of which help an organisation change its business processes and institute new ones where necessary. An example of a new business process that may be required is one that enables information access requests by data subjects.

Information technology underlies privacy-related and privacy-specific business processes. In an organisation, information technology usually facilitates the execution of business processes regarding private information. The particular information technologies used in a business process determines, to a large extent, what it is possible to do with private information. For example, the use of a database, as opposed to un-encoded, flat text files, makes it easier to interrogate data for specific information. Therefore, the choice of information technologies used affects the risk to data subjects'

³ Privacy-related business processes are those business processes which form part of the organisation's business operations, and which involve the use of private information.

A Digital Forensic Readiness Framework for Information Privacy Incidents

information privacy. It also impacts the DFR measures that may be implemented. Ideally, policies, procedures and standards are also required to govern the use and configuration of information technologies to ensure that they are used appropriately. As mentioned, a digital FORCFIPI is based on policy; however, it also addresses technology choices by mandating standards and procedures regarding the configuration and monitoring of the technology in use by an organisation.

Digital forensic investigations of information privacy incidents in an enterprise involve the information privacy context: privacy-related business processes, privacy-specific business processes, information technologies supporting the processes, policies that govern the processes, and the auditing and monitoring of the processes. The information privacy context, with the exception of information technology, expresses what is required by a privacy-specific approach for digital forensic readiness in addition to the traditional security-related approach. A digital FORCFIPI deals with all aspects of the information privacy context.

To help understand the rationale presented above, it may help to look at some cases in which a digital FORCFIPI is particularly useful. Consider the following cases:

- A data subject alleges a violation of his or her information privacy by the organisation itself. If the data subject takes legal action, a digital FORCFIPI will allow the organisation to conduct a more effective DF investigation that it can use in its defence. The investigation will be more effective as privacy-specific and privacy-related business processes and the related technology and policies would have already been set out explicitly and readily available to the forensic team. In the absence of these, much time and expense would be incurred by the forensic team to work out the applicable business processes, policies and technologies and the relationships between them. This is particularly true for large organisations where there are many business units, comprised of many departments, each that will have their own privacy-specific and privacy-related business processes. A FORCFIPI does not require the investigative team to possess expert knowledge about these business processes. It only requires that this information is on hand should the need to use it arise. As pointed out by Tan (2001, p.2) in Chapter 4,

A Digital Forensic Readiness Framework for Information Privacy Incidents

preparedness reduces the time taken to investigate an incident, which results in the greatest reduction of cost.

- An employee of the organisation is charged with violating the organisation's privacy policy in an internal disciplinary hearing. In such a case the organisation may conduct a DF investigation to present evidence against the employee in the disciplinary hearing. The investigation is likely to proceed in a more efficient manner if a digital FORCFIPI is already in place. This can be seen in the scenario of an employee that is authorised to access data via an application and then misuses the data contained within the application. A security-related DF capability may only require that access logs for the application be put in place. In this scenario nothing would seem remiss since the employee is authorised to access the data. A digital FORCFIPI, on the other hand, would go further by mandating that the employee's actions with the data are also logged by the application and that the logs are monitored. An additional advantage of a digital FORCFIPI is that it has value as a deterrent – employees are less likely to attempt information privacy violations if they are aware that a digital FORCFIPI exists and can be used against them.

6.3 Framework

In this section we describe the framework and the rationale for its design. The framework is a theoretical representation of a generic digital forensic readiness capability for dealing with information privacy violations within organisations. It thus aims to provide a basis upon which organisations can build a digital FORCFIPI. The framework has a hierarchical tree-like structure and we have labelled each level alphabetically starting at level 'A' as depicted in Figure 11 below. Within each level, each element is depicted by a block. Blocks have been labelled in numeric sequence from left to right. The framework can be seen in its entirety in Appendix B.

It should be noted that, per the definition of a framework given in Section 6.1, the tree structure of the framework consists of a variety of different elements (or blocks). Some blocks are business processes while some blocks are physical devices. Each element or block represents something that is required for DFR. Whenever a block is decomposed

A Digital Forensic Readiness Framework for Information Privacy Incidents

into other blocks in the next level, this indicates that what is shown in the next level is logically required based on the block above. The tree structure should not be read as a process flow diagram. If business process A is decomposed into business processes B and C, this merely indicates that business processes for B and C are also required. It does not mean that process A must split into separate processes for B and C. It may be that an organisation implements a business process for A which includes B and C without physically splitting process A. In this case the organisation has met the requirements of the framework and does not need separate processes for B and C. The same applies to policies. If a block containing policy A is decomposed into blocks for policy B and C, this merely indicates that the organisation should consider B and C in its policies. B and C may exist together in a single policy or both may be part of policy A. All that the framework requires is that the organisation takes into account the policies represented by the various blocks.

We discuss the framework moving from top to bottom.

6.3.1 Top Levels of the Framework

The starting point of the framework, depicted in Figure 11 as block A1, is an overall forensic policy, or organisational forensic policy, that has been approved by management. In an organisation, a forensic policy is required to guide the processes and procedures involved in, and supportive of, a DF investigation (Wolf 2004)(Noble et al. 2000, p.5). It also provides official recognition of the role of DF within the organisation (Wolf 2004).

We decompose block A1 into the blocks shown in level B in Figure 11. This decomposition symbolises the various phases of a DF investigation in Carrier and Spafford's model (Carrier & Spafford 2004) which was discussed in Chapter 3. Each phase is included in our framework to highlight the need for forensic policy to cater for each phase. As we are only interested in DFR we do not list all the phases. Rather, we show incident response in block B2 to illustrate the concept of multiple phases and abbreviate the remaining phases in block B3. It is important to note that the decomposition from level A to level B is logical and not physical. In other words, each

A Digital Forensic Readiness Framework for Information Privacy Incidents

phase of a DF investigation does not require a separate policy. All the phases may, for example, be addressed in a single forensic policy, such as the overall policy.

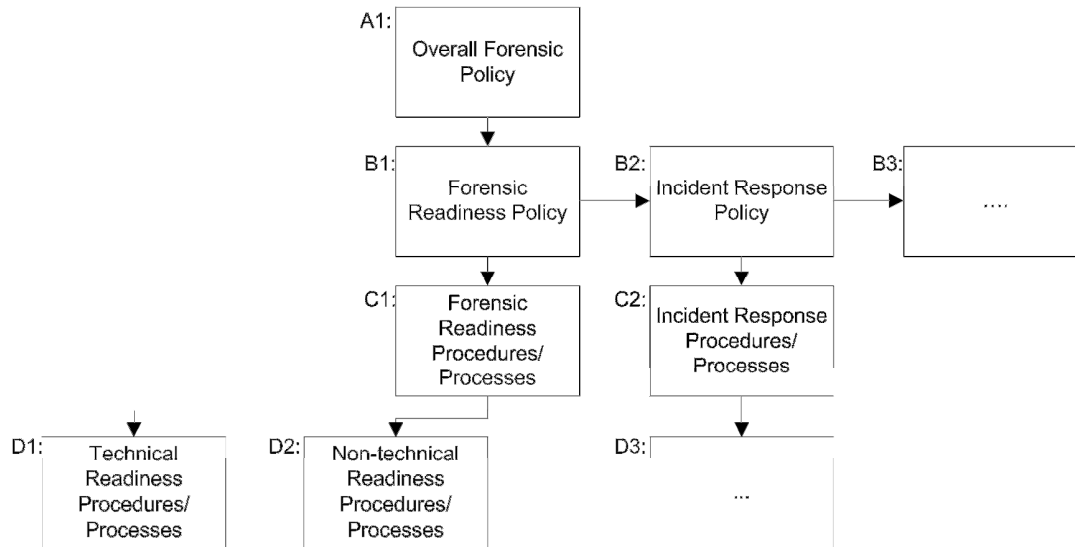


Figure 11 – Levels A to D of the framework

Level C in Figure 11 indicates that the policy in level B should be implemented as procedures or processes. Block C2 is, again, only shown for illustrative purposes. Our scope in this thesis is limited to DFR, therefore we follow the branches leading from block C1, namely DFR procedures or processes. This leads us to block D1 (Technical Readiness Procedures and Processes) and block D2 (Non-technical Readiness Procedures and Processes). Each of these two blocks is elaborated on in the following two sections.

6.3.2 Technical Readiness Procedures and Processes

Blocks D1 and D2 represent the technical and non-technical components of digital forensic readiness, which follows from the definition of DFR. The distinction between technical and non-technical aspects of DFR is also roughly analogous to the operations readiness and infrastructure readiness phases of Carrier and Spafford's Framework (Carrier & Spafford 2003, p.7) mentioned in Section 3.2.1.3. Rowlingson (2004, p.17-19) states that monitoring and auditing should occur as part of DFR in order to detect and deter incidents. Additionally, Rowlingson also requires procedures and processes to be in place to retrieve and preserve data in an appropriate manner. In Figure 12 we show this by splitting block D1 into blocks E1 to E3.

A Digital Forensic Readiness Framework for Information Privacy Incidents

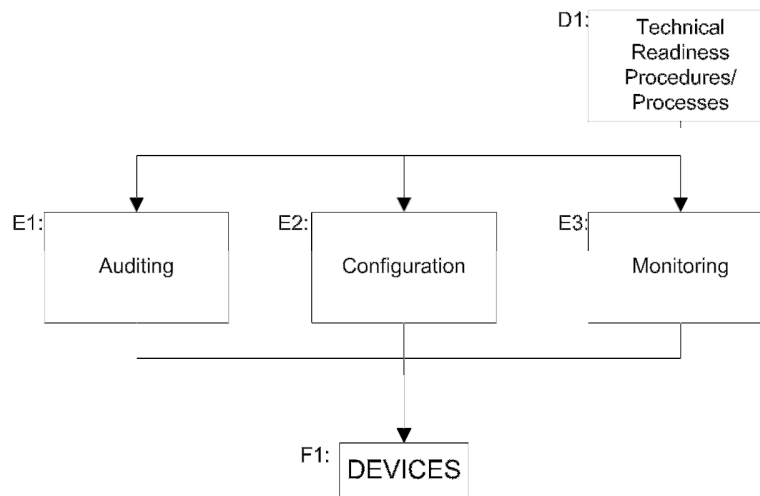


Figure 12 – Technical parts of levels D to F

We believe that configuration standards, procedures and/or processes should also exist. This is depicted in block E2. The primary reason for this is that if systems are not configured appropriately, it may not be possible to collect logs and other evidence from them at all, or in an efficient manner. Also, auditing and monitoring may not be possible, or particularly useful, if the correct configuration has not been applied to all the required hardware and software (Tan 2001). Take, for example, the cases of (1) a firewall that has not been configured to log certain events, and (2) a firewall and switch both configured to log events, but configured to use time servers that are not synchronised. In the first case, if the firewall is not logging the correct events, there will be no evidence to collect and these events will not be noticed in the monitoring or auditing processes. In the second case, it may be difficult to correlate events from the switch and firewall, thereby reducing the evidentiary value of any logs that are produced.

Blocks E1 to E3 merely indicate that monitoring, auditing and configuration should apply to the devices used in the appropriate business processes. In these blocks the term ‘devices’ is taken to mean both hardware and software. It is used as an abbreviation in the diagram as the complete framework contains a more exhaustive list, for example: networking devices, operating systems, databases, applications and mobile devices. Each of the devices is then sub-divided further in subsequent levels in the complete framework, which can be seen in Appendix B.

A Digital Forensic Readiness Framework for Information Privacy Incidents

6.3.3 Non-technical Readiness Procedures and Processes

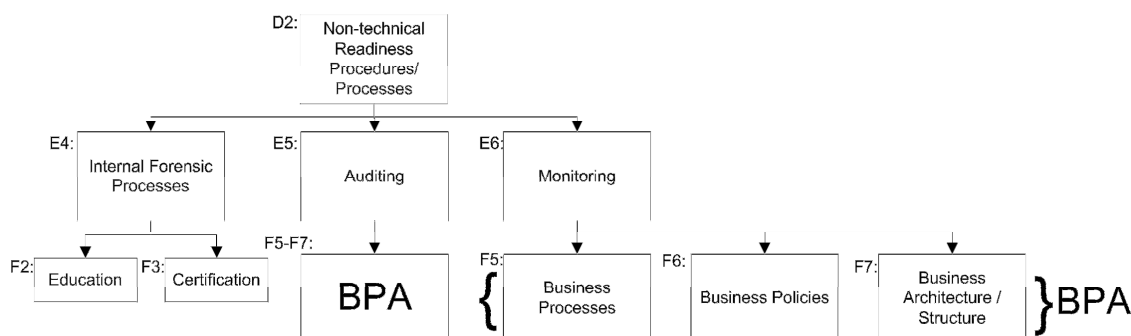


Figure 13 – Non-technical parts of level D to F

The branches from block D2 in Figure 13 are concerned with the non-technical aspects of DFR. Many of the DFR aspects that are pertinent to privacy are found in this part of the framework. The non-technical components of the framework are comprised of internal DF processes, auditing and monitoring, as shown in blocks E4 to E6.

The internal forensic processes in Block E4 are processes that are unique to the forensic team of an enterprise. An example of such a process is the education (Mohay 2005, p.159-160) of forensic team members (Block F4). When implementing a forensic readiness capability for information privacy incidents, it is important to educate forensic investigators (who are primarily trained in security) about information privacy laws. Forensic team members should also have the appropriate certifications (Block F5). These include certifications for conducting digital forensic investigations as well as privacy-related certifications (International Association of Privacy Professionals 2011). In the complete framework a Block F4 is also included as a child node of Block E4. Block F4 is entitled “Performance Appraisal / Investigation Review”. Block F4 highlights the need to review the performance of the DF team and any investigations that have been carried out (Rowlingson 2004, p.25). Blocks F2 and F3 are also only listed as examples and do not represent all the branches of block E4 in the complete framework.

Auditing and monitoring in the non-technical part of the framework, which is depicted in blocks E5 and E6 respectively, refers to the auditing and monitoring of business processes, policies and architecture. The business processes and policies envisaged here

A Digital Forensic Readiness Framework for Information Privacy Incidents

are only those that have a strong relevance to information privacy in the organisation. They are discussed in more detail later. Likewise, business architecture is limited to the structure of the business as it pertains to information privacy. Examples would include the creation of the chief privacy officer (CPO) role, or the creation of a multi-disciplinary team (Luoma 2006) consisting of staff from the office of the CPO, information security, forensics and the legal department. Business processes, policies and architecture are shown in blocks F5 to F7, respectively. They are also abbreviated as BPA as shown in the child node of Block E5.

6.3.3.1 Privacy and Business Processes

Figure 14 shows the decomposition of business processes into privacy-specific and privacy-related business processes from block F5 to blocks G1 and G2. As defined previously, privacy-related business processes are those business processes which form part of the organisation's business operations, and which involve the use of private information. Block G2 is an abbreviation of these processes since they are unique to each organisation and depend largely on the nature of the organisation's operations.

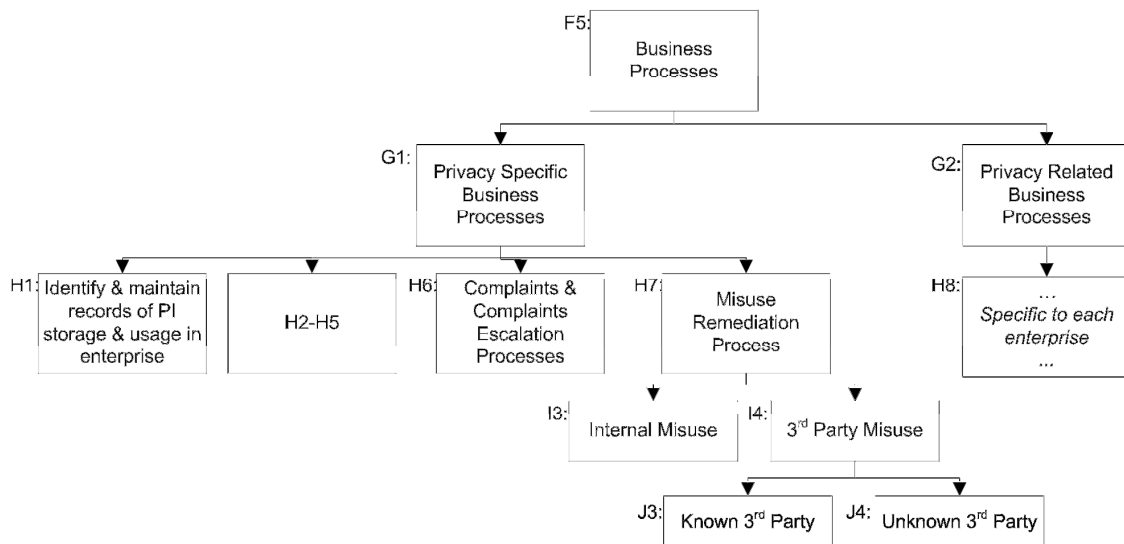


Figure 14 – Business processes in the framework

In a delivery company, for example, the process of capturing the details for a delivery to an individual is considered a privacy-related process. The reason is that the receiver's address is private information (the sender's details are also private information and

A Digital Forensic Readiness Framework for Information Privacy Incidents

perhaps even the sender’s relationship with the delivery company). Including privacy-related processes in the framework is important as it gives DF investigators immediate information about the business processes likely involved in privacy incidents.

Privacy-specific business processes, on the other hand, can be defined as those business processes that deal purely with information privacy. They ensure the actions required to protect, enforce, and further the information privacy rights of data subjects are in place within the organisation. In Figure 14 they are shown as the branches of block G1. Some of these processes have been omitted from the diagram due to the available space for the diagram. These can be seen in Figure 15 below. The privacy-specific business processes in the framework have been populated from the Generally Accepted Privacy Practices (GAPP) (American Institute of Certified Public Accountants & Canadian Institute of Chartered Accountants 2006) standard that has been promulgated by the American Institute of Chartered Professional Accountants and the Canadian Institute of Chartered Accountants as a guide for information privacy audits. It is necessary for organisations that are audited using the GAPP standard to adhere its requirements. This will entail the organisations having the privacy-specific business processes shown in Figure 15.

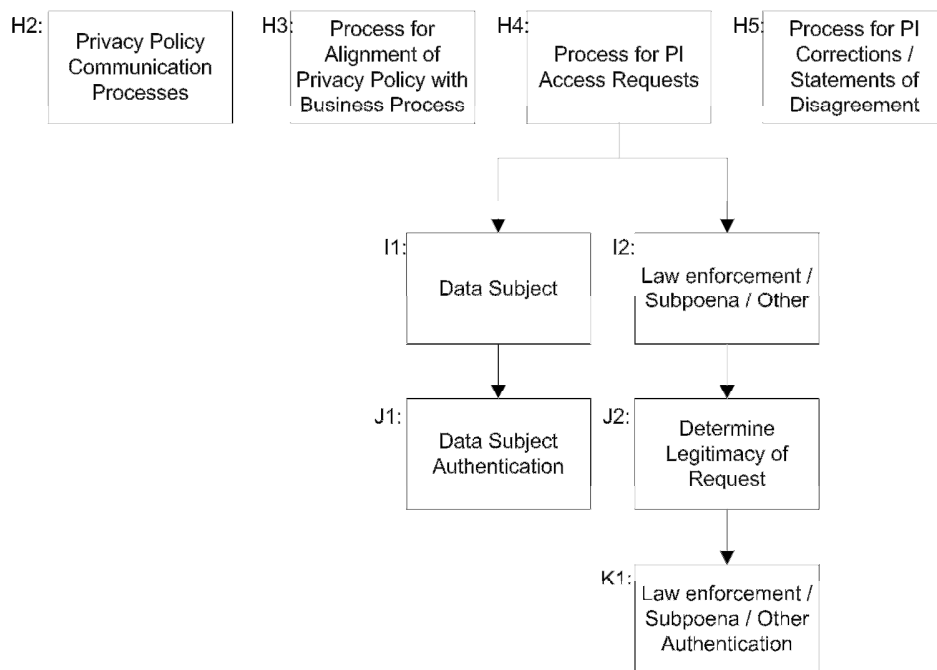


Figure 15 – Privacy-specific business processes H2-H5

A Digital Forensic Readiness Framework for Information Privacy Incidents

Block H1, seen in Figure 14, indicates that an organisation should have a business process in place that facilitates the identification of private information (PI). The location of records that contain PI should be recorded, as well as the type of information stored, for example, telephone numbers. The use of the PI should also be recorded. Furthermore, it is important that the business process ensures that such information is maintained – that is, it is kept current.

Block H2 in Figure 15 is self-explanatory. It shows that there is a requirement for a business process to communicate the organisation’s privacy policies to data subjects and to employees within the organisation. This is important especially when privacy policies change. Block H3 in Figure 15 seeks to ensure that business processes, both privacy-specific and privacy-related are aligned with the organisation’s privacy policies. The business process envisaged in Block H3 is one that involves regular communication between staff responsible for creating privacy policies and staff responsible for privacy-specific and privacy-related business processes.

In Block H4 a business process to allow outside access to PI is presented. Separate processes are required for data subjects wanting to access their PI, and non-data subjects who wish to access information about data subjects. These separate processes are indicated by the decomposition of Block H4 into Block I1 and Block I2 in Figure 15. Block I1 deals with access requests by data subjects. The business process to handle such requests involves a process to authenticate the data subject. The authentication of data subjects is shown as Block J1. The separate process to deal with PI access requests from non-data subjects is shown in Block I2. A non-data subject may represent a law enforcement agency, opposition in a legal case or some other individual or organisation with a legitimate right to access data subjects’ PI. Before providing a non-data subject with PI, the legitimacy of a request must first be determined – indicated in Block J2. For example, certain requests from law enforcement bodies may only be legal with an appropriate warrant. Once the legitimacy of the request has been ascertained, the organisation needs to authenticate the individuals requesting the PI. This is shown in Block K1. The reason for the authentication is to prevent social engineering attacks where individuals pretend to represent, say law enforcement, to obtain information.

A Digital Forensic Readiness Framework for Information Privacy Incidents

Social engineering is a technique used by hackers or other attackers to gain access to systems through obtaining the needed information from a person rather than breaking into the systems through electronic or algorithmic hacking techniques (Orgill et al. 2004, p.177).

A business process in which data subjects can correct their PI is recommended in Block H5 in Figure 15. Where a correction is not possible or there is a dispute, for example, regarding a data subject's credit rating, a statement of disagreement may be recorded. In this eventuality, the organisation does not change the information, but rather records that the data-subject disputes the accuracy of the information. This helps prevent inaccurate information about the data subject from being passed on.

The business process in Block H6 in Figure 14 is a business process for complaints by data subjects. It allows data subjects to complain about real or perceived breaches of their information privacy. It also makes provision for a complaint to be escalated to the management of an organisation. Escalation is necessary for complaints to be resolved where resolution is not possible at the first point of call for data subjects. This business process is important as it provides an opportunity for redress for data subjects where information privacy has been breached.

Block H7 in Figure 14 represents the misuse remediation business process. Misuse remediation is a term used to describe incidents in which PI is used in a manner that has not been sanctioned by the data subject. The framework divides misuse into internal misuse and third party misuse, which are displayed in blocks I3 and I4, respectively. Internal misuse refers to misuse by an individual or individuals in the organisation. It is treated differently to third party misuse, which refers to misuse by an individual or individuals outside the organisation. As shown in blocks J3 and J4, third party misuse is itself decomposed into misuse by known third parties and unknown third parties. Known third parties include business partners or outsource service providers, while an unknown third party may include a hacker.

The purpose of decomposing misuse remediation into the categories in the framework is to indicate that a different DFR process may be required for each category – for example,

A Digital Forensic Readiness Framework for Information Privacy Incidents

a readiness process to cater for privacy incidents between the organisation and business partners may include the following: the establishment of a joint forensic team at the outset of the partnership; arrangements to gain physical access to the business partner's servers in the event of an incident; and, an agreement over which servers may be examined forensically.

6.3.4 Business Policies

Figure 16 below shows the organisation's business policies. These are policies that provide guidance with regard to information privacy, information security and the disciplining of employees. Information security policies, shown in Block G4 are included since information security is necessary for information privacy (Burkert 1998, p.125). Disciplinary policies are also included in the framework because breaches of information privacy or security policies should result in disciplinary action that is commensurate with the nature of the infringement or breach. The disciplinary policies should therefore be aligned with the other policies. Where disciplinary policy is not stringent enough, employees are more likely to risk breaching the information privacy and security policies.

Privacy policies in the framework are split into an internal privacy policy for employees of the organisation, and privacy policies for data subjects. These are shown in blocks H9 and H10, respectively. The internal privacy policy sets out the guidelines for the acceptable use of data subjects' private information by employees. As such, it plays an important role in defining an information privacy incident, since such an incident usually occurs when the policy has been violated by an employee. It also makes clear the repercussions for employees if they do not adhere to the guidelines.

A Digital Forensic Readiness Framework for Information Privacy Incidents

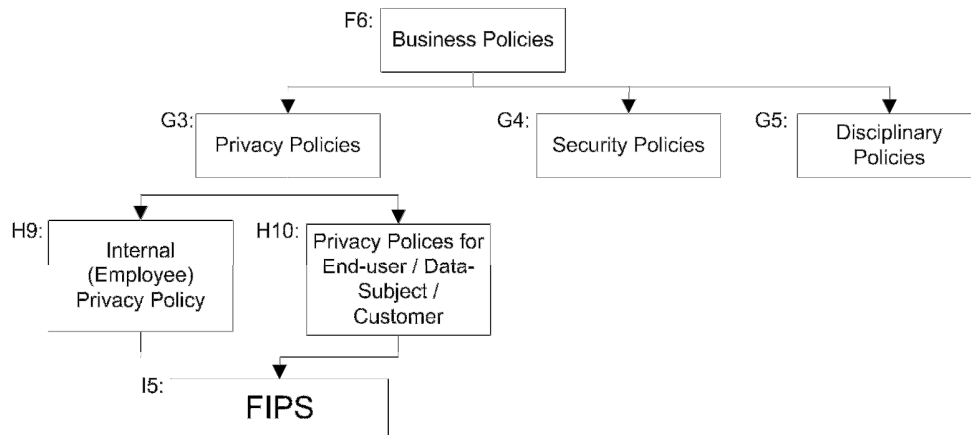


Figure 16 – Privacy policies in the framework

Privacy policies for data subjects are the policies that the organisation presents to data subjects. These policies inform the data subject about the organisation’s practices regarding their private information. Data subjects may then hold the organisation to these policies and institute complaints where they believe the organisation has not adhered to the policy. The policy is therefore useful to a forensic investigator tasked with investigating a complaint by a data subject.

In the framework both the internal privacy policy and privacy policies for data subjects are based on the FIPs because most information privacy law makes use of the principles contained in the FIPs (Gellman 1998, p.194). Other guidelines such as applicable laws may also be included here. Block I5 is an abbreviation for the FIPs. In the complete framework in Appendix B each FIP is listed in a separate block. This is to indicate that separate policies may exist for each principle in the FIPs. For example, an organisation may have a separate policy regarding consent by the data-subject for his information.

6.3.5 Organisational Structure

An organisation that wishes to use a digital FORCFIPI successfully requires certain roles and coordination between various functions within the organisation. This section of the framework, shown in Figure 17, illustrates these requirements.

A Digital Forensic Readiness Framework for Information Privacy Incidents

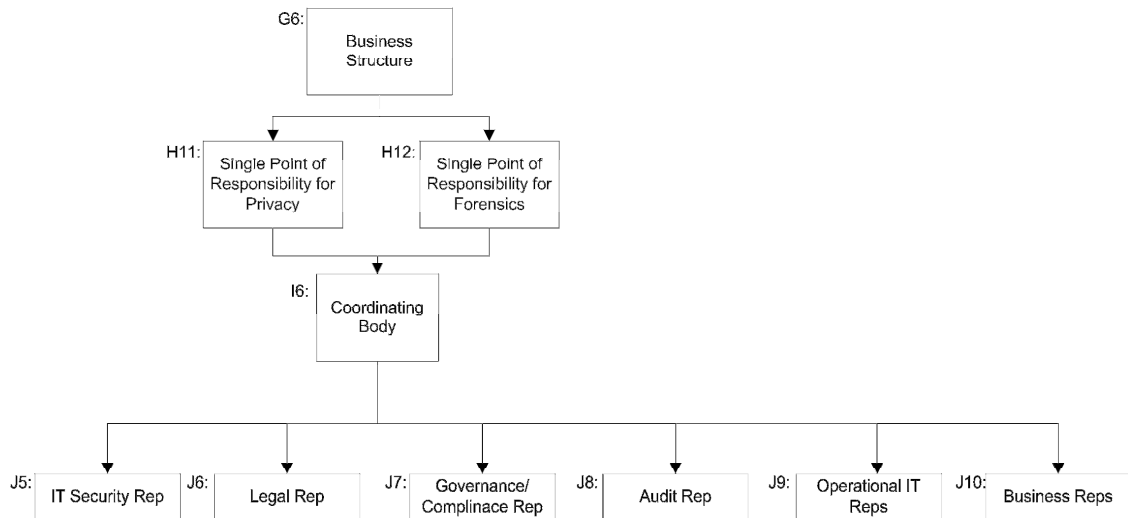


Figure 17 – Organisational structure

As shown in Block H11, the framework requires that a single individual holds the ultimate responsibility for information privacy within the organisation. This ensures that accountability is not diminished or diluted by having a number of people share responsibility (Baccarini et al. 2004, p.288)(Shenhar & Renier 1996, p.27). Typically, in a large organisation such an individual is known as the Chief Privacy Officer (CPO), however, the framework does not mandate specific job titles. The framework only requires that the overall responsibility is officially part of a single individual’s job description. An organisation may make the overall responsibility for information privacy part of the Chief Legal Officer’s job, since efforts to ensure information privacy are often done to comply with legal requirements. An organisation may also vest the responsibility for information privacy with the Chief Security Officer due to the overlap of the duties involved in ensuring information security and information privacy.

A similar role, shown in Block H12, is required for DFR. In order to ensure the correct working of the framework, the information privacy and DFR functions need to work in conjunction with each other. The framework therefore mandates a coordinating body that not only coordinates the information privacy and DFR functions, but also includes representatives from the other functions that are required by the framework. These other functions are shown in Blocks J5 to J10. As already mentioned, information security is necessary to achieve information privacy and is therefore included in the coordinating

A Digital Forensic Readiness Framework for Information Privacy Incidents

body. A representative from the legal department of the organisation is necessary since information privacy policy and practices should be aligned with the relevant information privacy laws. If the organisation has a corporate governance department, a representative should also be part of the coordinating body because information privacy decisions can affect corporate governance (Pangalos et al. 2010, p.15). A representative from the internal audit function is mandated by the framework. The reason for this is that audits may identify deficiencies in, or the absence of, controls that are necessary to maintain information privacy or a DFR capability. It is worth noting that Pangalos et al. (2010, p.15) also motivate for the audit and DFR functions of a business to work in a more closely integrated fashion. Representatives from the information technology (IT) department that deal with IT operations are also required since privacy-related business processes will most likely make use of the IT services and infrastructure they administer. Lastly, representatives from business departments that are involved in privacy-related business processes are needed in the coordinating body. Their presence in the coordinating body is necessary since any changes to privacy-related business processes may affect the way their departments operate and may also have cost implications for their departments. A method for calculating such cost implications is presented in the next chapter.

6.3.6 Summary View of Framework

In the previous sections we described our framework as a tree structure in which the nodes represent all the items required in an ideal implementation of a digital FORCFIPI. This single and large framework can, however, be viewed in a compact, summarised form that splits the framework into five components as seen in Figure 18.

A Digital Forensic Readiness Framework for Information Privacy Incidents

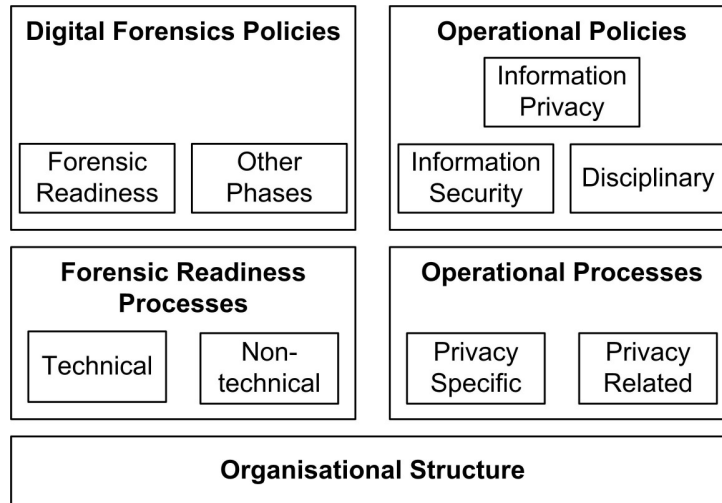


Figure 18 – Compact view

The five components are Digital Forensics Policies, Operational Policies, Forensic Readiness Processes, Operational Processes and Organisational Structure. Each of these components also represents a tree structure, though they are shown as blocks in Figure 8 for illustrative purposes. In the reorganised, summary form, the framework is easier to use and easier to discuss from a high level.

The Digital Forensics Policies component refers to policies specifically regarding digital forensics that are adopted by the organisation. The Digital Forensics Policies component represents the node for the Overall Digital Forensics Policy in Block A1 of the larger version of the framework shown in Figure 11 earlier. It also encompasses all the blocks in Level B of Figure 11.

Operational Policies refer to policies that are necessary for the protection of information privacy during the operations of the organisation, and which are not digital forensics-specific in nature. These policies are the organisation's Information Privacy Policy, Information Security Policy and Disciplinary Policy as shown previously in Figure 16.

Digital Forensic Readiness (DFR) Processes are the business processes that are performed specifically for the purpose of DFR. The business processes comprise of the technical and non-technical Processes discussed in earlier Sections 6.3.2 and 6.3.3, respectively.

A Digital Forensic Readiness Framework for Information Privacy Incidents

The Operational Processes component of the framework describes privacy-related and privacy-specific business processes, which were discussed in Section 6.3.3.1 above.

The Organisational Structure component of the framework specifies roles within the organisation that should be fulfilled in order for the framework to function optimally. This was discussed in the previous section.

6.4 Discussion

In the previous section we discussed the structure of the framework. In this section we discuss the framework and how it incorporates information privacy protection. We also provide a high-level explanation of how it can be implemented. We restrict ourselves to a high-level discussion since this thesis focuses on the structural rather than implementation details of the framework.

The primary aim of our framework is the inclusion of information privacy protection in the DFR capability of an organisation. In order to incorporate information privacy into our framework we have used the GAPP standard. In our review of the literature it was the only document we found that provided comprehensive guidance on the operational or practical requirements necessary for information privacy protection. Following the accepted notion that security-related DFR is not possible without basic information security processes such as logging and reporting in place (Tan 2001)(Wolf 2004), we hold that the same is true for a digital FORCFIPI – basic information privacy practices are required by an organisation in order to implement a digital FORCFIPI. In our framework we specify these basic practices from the GAPP standard. Organisations with a higher level of maturity in information privacy protection, that is, executing these practices, are therefore more likely to have a better digital FORCFIPI than those that have a lower level of maturity (Reddy & Venter 2007).

The GAPP standard, furthermore, is grounded in the FIPs and is thus applicable in most countries that have information privacy protection legislation. The framework is therefore also applicable in such countries.

A Digital Forensic Readiness Framework for Information Privacy Incidents

The framework has also included established ideas from security-related DFR (Endicott-Popovsky et al. 2007)(Rowlingson 2004)(Wolf 2004)(Yasinsac & Manzano 2001), namely a policy and process approach to DFR. Indeed, the framework's contribution is the combination of these established ideas with information privacy protection measures and in defining the relation between the policies, processes and procedures with respect to information privacy incidents. While the principal aim in the design of the framework is the inclusion of information privacy protection in the DFR capability of an organisation, the framework itself is intended primarily as an idealistic, or theoretical, guide to an organisation for a coordinated approach to a digital FORCFIPI. The framework will, thus, have to be realised in a real-world organisation. As an idealistic or theoretical framework it is unlikely that it will be implemented entirely 'as-is' in a real world organisation. This is because of the large number of requirements that exist in the framework and the fact that cost-constraints may limit a full implementation. Policies and processes that exist as separate elements in the framework may be combined if they already exist in a combined form in the organisation. It is also possible for the organisation to omit policies and processes; however, this introduces a risk that some aspects of information privacy protection may not be covered by the digital FORCFIPI.

Since DFR is defined as being a corporate goal (Rowlingson 2004, p.4), the first step to implementing the framework is to obtain senior management approval. Similar approval is also required for all of the policies in the framework, especially the privacy and forensic policies as these are vital for a digital FORCFIPI. Certain business processes, however, may only require approval from lower level management responsible for executing the processes. For example, the process for communicating privacy policies throughout the organisation may only require approval from middle management in the internal communications department.

Upon the necessary approvals, the privacy-related and privacy-specific business processes should be analysed to determine the information technologies used in each process. To illustrate what is meant by this, consider a privacy-related business process that involves a data-subject e-mailing private information to an employee in the organisation. The employee then opens the e-mail and enters the private information into

A Digital Forensic Readiness Framework for Information Privacy Incidents

an application that stores it in a database. The technology of interest to the DF investigator in this case consists of: the mail server that receives the data-subject's e-mail; the employee's e-mail client used to download the e-mail; the operating system of the employee's computer; the application and the database it stores information on; and finally, the operating system of the database server. Where practical and cost-effective, each item should exist in the devices section of the framework, along with a process for configuration, monitoring, auditing, and forensic analysis. Risk and cost-benefit analyses (Rowlingson 2004, p.13) may be used to determine which items to include. As mentioned previously, the next chapter discusses a methodology for carrying out such cost-benefit analyses.

An exercise similar to the mapping of technologies to business processes, which was discussed in the previous paragraph, can be conducted with privacy policies and privacy-specific business processes. This will ensure that a forensic investigator knows which policies are relevant for incidents that involve a particular business process or processes.

6.5 Conclusion

In this chapter we have presented the structural aspects of a digital forensic readiness framework for information privacy incidents. The framework is based upon prior work on DFR that has identified the necessity for policies, procedures and processes. It also encompasses information privacy imperatives through the incorporation of the FIPs, standards such as GAPP, and existing work in the information privacy literature. We have taken these concepts from DFR and information privacy and combined them to form the framework. The framework, therefore, shows the relevant items from each discipline and their relation to each other. As such, it is able to serve as guide to organisations wishing to develop a digital FORCFIPI.

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

7 Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

7.1 Introduction

In the previous chapter we discussed how a digital forensic readiness capability for information privacy incidents (FORCFIPI) can mitigate the risk to organisations from information privacy incidents. We noted that a digital FORCFIPI that is developed or executed in an ad-hoc manner is not as likely to succeed as one that involves the coordinated participation of individuals and departments throughout the organisation (Endicott-Popovsky et al. 2007, p.8). The coordination of organisational resources to attain an acceptable level of DFR, thus, becomes a management challenge. Cost is a significant factor in implementing or managing a digital FORCFIPI because implementation and management decisions are usually made with respect to cost constraints and risk assessments. Indeed, Rowlingson (2005, p.7) notes that the “critical question for successful forensic readiness is what can be performed cost effectively”. Organisations are bound, therefore, to stay within their cost constraints when implementing and managing a digital FORCFIPI. The traditional means of accounting for cost in organisations are not adept at providing cost information for specific activities (Brimson 1991, p.7-11)(Gunasekaran 1999, p.118-9). This makes it difficult for organisations to use cost as a criterion when making decisions about which elements of the digital FORCFIPI to implement, despite cost being a necessary criterion. The following questions thus arise: Is it possible to determine the cost of the specific activities required in a digital FORCFIPI? If so, how should an organisation determine such costs?

In this short chapter we attempt to answer these questions by discussing how Time-Driven Activity-Based Costing (TDABC), as discussed in Chapter 5, can be used to determine the cost of the specific activities required in DFR programmes such as a digital FORCFIPI. By providing activity-specific cost information, TDABC allows an organisation to weigh costs against risks when making decisions about the management and implementation of a digital FORCFIPI. Furthermore, it is often the case with information privacy that organisations do not have the option of omitting parts of the

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

framework due to legal or regulatory obligations. In this case, TDABC enables organisations to accurately calculate the cost of regulatory compliance. Organisations are, therefore, in a position to make accurate provision for these costs during their budgeting or financial planning processes. They are also better able to manage business processes involved in a digital FORCFIPI since it is more difficult to manage processes when the costs associated with the processes are not well defined (UcedaVelez 2008, p.62).

A simulation to demonstrate the concept of TDABC applied to DFR-related business processes is presented in the next chapter. What follows in this chapter is a section on the state of costing in DFR and a section containing a high-level discussion on the use of TDABC in implementing and managing a digital FORCFIPI.

At the time of writing this thesis, the content of this chapter was accepted for publication in the journal *Information Systems Frontiers* (Reddy et al. 2011) and published “online first”. No further information on which volume and issue the article would be published in was provided by the journal, therefore the citation is to the Digital Object Identifier (DOI) provided by the journal.

7.2 Costing in DFR

In this section we describe the results of our literature survey of related work. Our survey looked at work conducted on determining the cost of DFR. We also reviewed literature regarding the use of TDABC and activity-based costing (ABC) to determine the cost of security, privacy and DFR programmes and activities in organisations. Literature on the return on security investment (ROSI) was also reviewed for related approaches to determining costs. Finally, we consulted related work on risk assessment and on cost analysis.

Our literature review also did not reveal any work dedicated to determining the cost of DFR. Rowlingson (2004, p.5) mentions that the cost of a DFR programme must be taken into consideration, but does not present any methods for determining these costs.

No work was found on the use of TDABC applied to the field of digital forensics, or indeed to information technology in general. We believe this is due to the fact that the

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

concept is a relatively new one. There is, however, a large body of literature regarding the use of activity based costing (ABC) in a number of diverse fields, such as medicine (Glick et al. 2000) and the military (Jones 1998), where it has been adopted by the US Army. While we found no literature regarding the use of ABC in DFR, we did find a single instance of its use in information security – a report in which ABC was used to calculate the cost of security breaches (Ponemon 2006). ABC has also been used within the context of information technology to determine the cost of: software development (Ooi & Soh 2003), information technology services (Beekman 2007; Gerlach et al. 2002) and e-Business customer profitability analysis (Iltuzer et al. 2007).

Return on security investment (ROSI) literature generally focuses on determining the optimal amount of money to spend on information security given a certain level of risk (Mercuri 2003)(UcedaVelez 2008). Risk assessment literature is closely related to ROSI but concentrates more on the determination of risk and also on cost-benefit analysis (Butler 2002)(Stoneburner et al. 2002). Neither ROSI nor risk assessment literature provide detail on accurately determining cost. Our work, in contrast, is not concerned with determining the optimal amount to spend on DFR and information privacy. We focus instead on accurately determining the amount that has been spent, using TDABC as our method of choice for making this determination of cost.

(6) $ROSI = \frac{S - T}{T}$, where S = sum of avoided loss and T = total cost of security measures

In this equation it is clear that the precision of the ROSI calculation is dependent on accurate values of S and T since ROSI is a function of the variables S and T. TDABC can be used as a tool to calculate more accurate values for S and T, and therefore more accurate values for ROSI.

The work which was found to be most closely related to ours was the Incident Cost Analysis and Modeling Project (ICAMP) (Committee on Institutional Cooperation Security Working Group 1988) and its follow-up project I-CAMP II (Committee on Institutional Cooperation Security Working Group 2000). The ICAMP project aimed to develop a cost analysis model for security-related incidents, while I-CAMP II

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

concentrated on improving the cost analysis model in ICAMP and developing a classification scheme for security incidents.

The ICAMP projects were designed to be applied specifically to IT security breaches and to look at universities in particular. While TDABC, has a broader application, namely to information privacy, security and DFR in any industry, it is not difficult to generalise the ICAMP methodology for industries other than universities. It is, however, more difficult to use the ICAMP methodology to calculate costs other than incident costs, since calculating incident costs was the focus of the ICAMP models. TDABC is used to calculate incident costs as well as the cost of any other activities or business processes – for example, it is used to calculate the costs of business processes involved in privacy regulatory compliance. ICAMP does not cater for such cost calculations.

Another important difference, and advantage over ICAMP, is that TDABC is able to allocate the cost of ownership of equipment and any other expenses to the activities that consume them. This provides management with information as to the extent to which equipment or other expenses are being utilised from a cost perspective. The ICAMP models, on the other hand, include only the replacement cost for equipment and do not perform allocations for equipment use during incidents. ICAMP also does not factor non-productive time into its estimation of hourly personnel costs, which TDABC does.

In the section that follows we discuss the combination of TDABC and our digital FORCFIPI framework.

7.3 Combining TDABC and the Digital FORCFIPI Framework

The implementation and management of a digital FORCFIPI are significant undertakings. Both the implementation and the management of a digital FORCFIPI require the coordination of multiple resources and staff across departmental boundaries. Similarly, both are subject to budgetary or cost constraints that must be known upfront in the case of an implementation, and as close to ‘on-demand’ as possible in the case of managing a digital FORCFIPI. TDABC can be used in both instances to provide cost information that allows management to make more informed decisions. TDABC is particularly well

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

suited to determining cost in a DFR programme or digital FORCFIPI since a digital FORCFIPI largely consists of a series of well defined activities.

7.3.1 Implementation

An organisation that decides to implement a digital FORCFIPI should not decide on the DFR measures to be implemented in an ad-hoc manner. Implementation decisions should be based primarily on an assessment of the risks to the organisation determined through a risk assessment exercise (Rowlingson 2004, p.9). The risk assessment exercise should consider all relevant risks, including privacy risks, for which a separate privacy impact assessment (PIA) may need to be carried out (Stewart 1999). Legal requirements and the risk associated with non-compliance should also be taken into account during the risk assessment exercise. A risk assessment should be used to highlight the areas of greatest risk and, ideally all the DFR measures applicable to these areas should be implemented. In an ideal situation cost constraints are not a factor to consider. In most real-world situations though, cost constraints must be considered since the implementation of a digital FORCFIPI in an organisation would most likely occur in an environment with fixed budgets. A cost versus risk analysis is thus required to ensure that the most risky areas are covered within the available budgets. TDABC can be used as a cost estimation technique to determine the implementation cost of various DFR measures thereby assisting in the cost versus risk analysis. This is also useful in calculations regarding the return on security investment or ROSI.

Some DFR measures can not be omitted in an implementation because they are required by law. Using TDABC to work out the costs related to these parts enables the business to determine precisely the cost of compliance with the law, otherwise known as regulatory compliance. The fact that regulatory compliance is mandatory can be used to motivate for increased budgets to meet the associated costs. It can also be used to provide an accurate indication of the impact of regulatory compliance on operating profits.

Kaplan and Anderson (2007b, p.15) note that “the time-equations in TDABC provide managers with a capability for simulating the future”. Since the equations contain the primary factors for determining cost, so-called “what-if” analyses may be conducted for

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

different scenarios. We show how such “what-if” analyses can be performed in the next section. We also present a simulation, in the next section, which can also help an organisation draft realistic budgets. As mentioned earlier, the implementation of a digital FORCFIPI involves multiple departments or business units. The use of TDABC and simulation makes the cost to each department or business unit more transparent. This is important from a budgeting perspective as it allows departments or business units to balance any extra demands for resources due to a digital FORCFIPI implementation with other items in their budgets. Simulation also allows management to make more informed decisions about the outsourcing of any new activities or business processes.

Thus far we have not made a distinction between organisations that implement a digital FORCFIPI with some level of DFR practices already in place and those that implement a digital FORCFIPI without any DFR practices in place. Organisations that have existing DFR practices may be at an advantage over organisations that do not. Such an advantage may be present if existing practices bear some similarity – in the nature of the processes or resources involved – to practices that are required by the new digital FORCFIPI. The reason for this is that similarities between existing and potential DFR practices allow organisations to use historical data from existing practices for their cost calculations. This can improve the accuracy of cost estimations (Heitger 2007). Where there is a significant difference between existing and potentially new DFR practices, organisations with such existing practices enjoy little advantage over organisations without any existing practices.

Organisations that have no existing DFR practices and who wish to estimate the cost of potentially new DFR practices using TDABC, face the challenge, as in traditional costing, of accurately estimating costs with no historical basis. In this instance, TDABC is one of many cost estimation techniques that can be used. Unlike the case of cost management, in the case of cost estimation, we have found no literature on the effectiveness of TDABC relative to other cost estimation techniques. However, given that, as a cost estimation technique, ABC has been recognised as more accurate than traditional cost estimation techniques (Qian & Ben-Arieh 2008, p.805)(Sun et al. 2007,

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

p.4064), we surmise that TDABC may present similar benefits since it was designed to improve the accuracy of ABC.

The decision to implement TDABC itself, however, should be the outcome of a cost-benefit analysis. An organisation should consider the accuracy of existing cost management methods and systems in place and weigh this against the cost of implementing TDABC. It is possible that the potential gain in accuracy of TDABC over an existing method or system may not be worth the cost. Likewise, where there is no existing system or method, other methods may prove less costly or faster to implement.

There are a number of organisational factors that must also be considered before implementing TDABC in a large organisation. While a cost-benefit analysis may suggest the use of TDABC, these factors should also be assessed. Some of these factors have been identified in studies of ABC; however, we believe they apply equally to TDABC. Malmi (1997) notes that implementation projects must have top management support to ensure success. He also cautions that the differing needs of corporate headquarters and the local level where implementation occurs, be taken into account. Costs are often borne at the local level while the benefits are reaped at a higher level which may cause resistance to implementation (Malmi 1997, p.474). Again, top management support is required to overcome this resistance.

Organisational culture, particularly in technical environments, is also cited as a concern by Malmi. Staff without an appreciation of management accounting may not be sensitive to the need for it. In this regard Gosselin (2006, p.666) points out that if organisational learning is taken into account this may help implementations, especially in non-accounting environments. According to Gosselin multifunctional teams, in which accountants work with operational staff, are also required for success in implementations.

7.3.2 Management

Once an implementation is already in place, TDABC may bring all the advantages of an activity-based cost system to bear on the operation of a digital FORCFIPI. Management is better able to plan, control operations, and make informed decisions (Garrison et al.

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

2006, p.4) based on detailed activity-level information provided by TDABC. Specifically, the performance and cost information associated with the DFR-related activities is made evident and clearer. Management is more likely to be able to determine how these DFR-related activities impact on budgets and identify the reasons for over or under-expenditure. Inefficiency by employees, in resource usage or in the design of business processes is therefore more easily identified and corrected. The resultant transparency in activity-related costs means that the decisions of managers are also under greater scrutiny. In ABC implementations, this increased scrutiny has resulted in resistance to the use of ABC by managers (Malmi 1997, p.473). It is likely, therefore, that a similar reaction is possible in the case of TDABC. We believe this is an organisational behaviour issue that can be overcome through sufficient buy-in and enforcement at senior management and executive level.

Another issue that needs to be taken into consideration during the management of TDABC is how the distribution of organisational power may change. Malmi (1997) cites a number of authors that state that the use of a cost management system implies “a distribution of power among those who design, use and are affected by others’ use of them” (Malmi 1997, p.472). Top management need to be aware of any adverse changes in the distribution of power within the organisation to minimise resistance to the use of TDABC.

Kaplan and Anderson (2007b, p.24) point out that the extensive use of enterprise resource planning (ERP) systems in large organisations makes the integration of dedicated TDABC systems easier. In fact, Szychta (2010) states that where TDABC is not coupled with integrated information systems, such as ERPs and data warehouses, TDABC may not be sufficiently effective. The reason is that ERPs capture business process and activity information as well as provide access to cost and resource information. Integrated ERP and TDABC systems can allow management access to real-time information on-demand. This means that managers in security, privacy, digital forensics and other departments that may be involved in a DFR programme can review risk versus cost decisions as conditions change and take appropriate action. The decisions made by managers in these areas are often time-sensitive, making this an important advantage.

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

In the discussion thus far we have pointed out the potential of TDABC for altering decisions or actions in a DFR programme. Malmi (1997, p.469), however, points out that an activity-based cost system, such as TDABC “may be successful even when its results do not require any decisions or actions to be taken”. He states that the reduction in uncertainty provides a better basis to make decisions and this means that TDABC “may be of great value even without consequent actions, and without a change in an intended decision” (Malmi 1997, p.475). We endorse this belief that an activity-based cost system has an intrinsic value and does not derive its value purely on the basis of changes in decisions or actions. The ability to validate existing decisions and courses of action, we believe, is just as important.

From the discussion above it appears that where TDABC is appropriate for an organisation and DFR programme activities are chosen and managed on the basis of risk versus cost decisions, TDABC and a DFR work naturally with each other. While Kaplan and Anderson (2004) claim to have successfully implemented TDABC in 100 companies and Dalci et al. (2010) and Everaert et al. (2008) have demonstrated successful TDABC implementations, we have found no examples of TDABC applied to DFR. Accordingly, in the following chapters we show through analysis and simulation how TDABC and DFR programmes may work well together.

7.4 Conclusion

In this brief chapter we addressed the challenge of managing costs in a digital FORCFIPI. Since cost forms an integral part of decision making in the implementation and management of a digital FORCFIPI, we proposed and then discussed the use of TDABC to determine costs that can be used in the decision-making process. TDABC provides the ability to measure cost at the level of tasks and activities, which allows management to define activities or tasks it wants to measure, and use these as measurements to determine cost and performance. This is in line with the “widely accepted management principle that an activity cannot be managed well if it cannot be measured” (Savola 2007, p.28). In this regard TDABC differs from traditional costing methods that do not provide cost

Using TDABC to Manage DFR for Information Privacy Incidents in Large Organisations

information at the activity and task level cost. It also differs from ABC in that it is less costly and simpler to implement.

While we have provided a discussion on implementing TDABC, it should be noted that detailed empirical research based on an actual implementation of TDABC with regard to DFR processes is required to get a full or deeper understanding of the organisational issues mentioned in the chapter. Such research, however, is out of the scope of this work since a large component of it involves the academic discipline known as organisational behaviour. The research itself is also too large an undertaking to include within this work.

In the next chapter we describe simulations performed to test the assertion that TDABC can be used to determine costs and also to assist in the decision-making process.

8 TDABC and a Digital FORCFIPI – Information Query Simulation

8.1 Introduction

In this thesis we describe how TDABC can interact with a digital FORCFIPI by presenting two simulations and an analysis technique. Since a digital FORCFIPI consists of both technical and non-technical business processes, we simulate both technical and non-technical business processes. In this chapter we simulate a scenario that involves a business process which is non-technical in nature. In the following chapter we consider a technical business process and also present an analysis technique.

The simulation performed in this chapter involves an information query by a data subject. The business process to address an information query is defined in our digital FORCFIPI as a privacy-specific business process. The simulation is presented in the following section and includes a description of the simulation environment, the TDABC model used in the simulation, the statistics used and, finally, the results and insights gained in performing the simulation.

8.2 Simulation

The simulation of activity-based costing systems in general is a technique that has been used by numerous authors (Glick et al. 2000)(Helberg et al. 1994)(Jones 1998)(Leslie Gardner et al. 2000)(von Beck & Nowa 2000). In this section we describe our simulations involving the combination of TDABC and DFR-related business processes. Simulation was chosen to validate the combination of TDABC and a DFR programme as the large organisations with DFR programmes in place in South Africa, typically banks, were not prepared to take part in a study for security reasons. Below we discuss the simulation environment as well as the details and results of each simulation.

In the simulation we simulated an information query by a customer – that is, a query by a customer regarding the customer’s personal information held by the organisation. It is mandatory in European Union (EU) (European Parliament 1995) law for organisations to provide customers their information in response to such queries. As mentioned in

TDABC and a Digital FORCFIPI – Information Query Simulation

Chapter 2, South Africa currently has no comprehensive information privacy law such as in the EU. South Africa does, however, have a Promotion of Access to Information Act (PAIA) (South Africa 2000) that provides individuals the right of access to their information (South Africa 2000). According to Tilly and Mayer in Memeza (2006, p.11) the PAIA, is not used often, owing to a lack of awareness, clarity in the Act itself and the cost of enforcing non-compliance. Nevertheless, customers do have the right to access their personal information.

8.2.1 Simulation Environment

Our simulation was conducted in Microsoft Windows XP using the Microsoft Office Excel 2003 spreadsheet (Excel) and SPSS PASW Statistics 17 software (SPSS) (SPSS 2009). SPSS is a statistical analysis package that has its own fourth-generation programming language, known as SPSS Syntax. SPSS Syntax can be used to control SPSS programmatically, as opposed to using SPSS's graphical user interface (GUI).

The TDABC model for the simulation was developed in Excel and SPSS was used to generate the random data required for the simulation. Microsoft Visual Basic for Applications (VBA) was utilised from within Excel to develop a GUI program to write simulation parameters to an SPSS Syntax file. The GUI for the simulation can be seen in Figure 21 in Section 8.3.2 below. The VBA program was then used to execute the SPSS Syntax file from the command line interpreter using SPSS's 'background mode', an execution mode that runs SPSS as a background process. Once executed, the SPSS Syntax program produced output in the Excel file format. The VBA program was then utilised to load the output from the SPSS Syntax program into Excel. The TDABC model in Excel then automatically updated itself. This was because the formulae in the TDABC model contained links to the SPSS output. A diagrammatic representation of the simulation is shown in Figure 19 below.

TDABC and a Digital FORCFIPI – Information Query Simulation

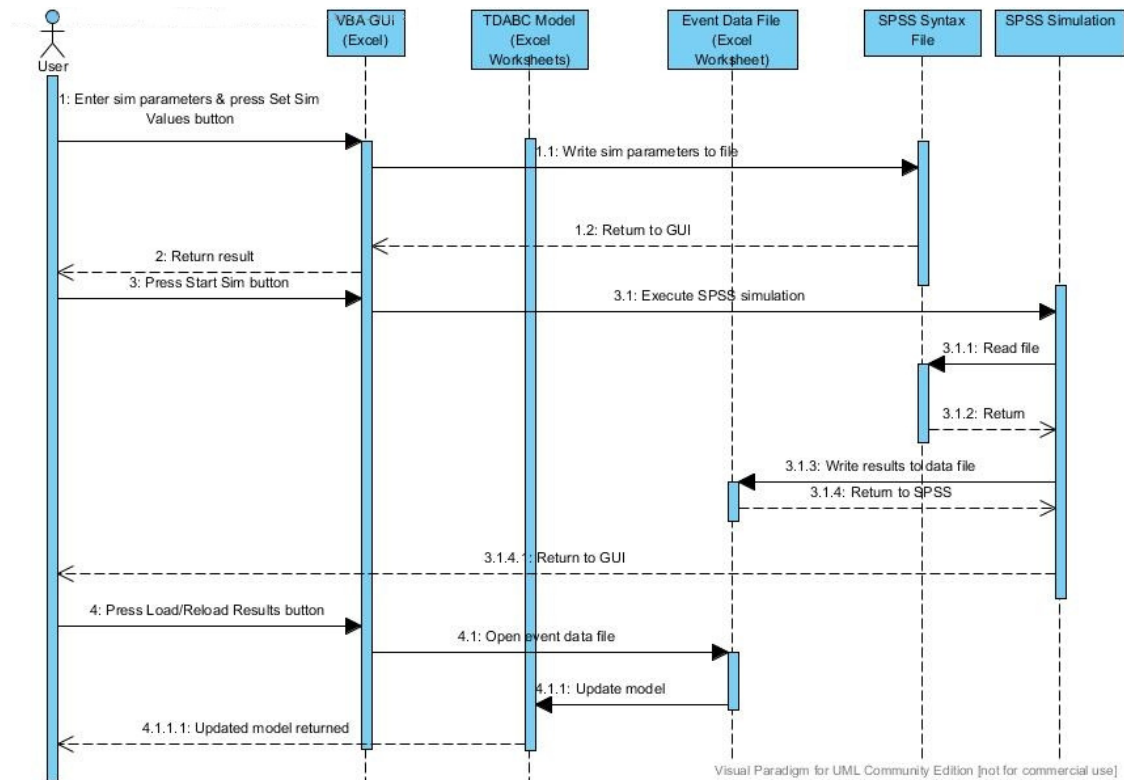


Figure 19 – UML sequence diagram describing the simulation⁴

8.2.2 General TDABC Model

We utilised a generalised TDABC model in Excel which was populated with the specific data for each scenario being simulated. The model allowed for the specification of: the cost of resources, including human resources; activities and tasks, as well as variations to activities; detailed capacity cost rates; and cost driver rates for the activities and their variations. The total yearly cost calculated in the model was determined based on the volume of the activities generated by the statistical simulations in SPSS.

The activities simulated required resources from multiple departments, or resource pools, within the organisation. Also, the activities themselves consisted of numerous tasks. The time taken to complete each task was defined and a capacity cost rate was calculated for the resources from each resource pool. Using these capacity cost rates and times, the cost driver rate for each task was determined. The cost driver rate for the activity was then

⁴ As noted in the image, the UML diagram was created using the Community Edition of Visual Paradigm for UML (Visual Paradigm 2011)

TDABC and a Digital FORCFIPI – Information Query Simulation

calculated by finding the sum of the cost driver rates for each of the tasks that constituted the activity. This follows from our definition in Section 5.2, of an activity as an aggregation of tasks. Equation (4) in Section 5.3.2 does not hold in this case as there is no single capacity cost rate to use. We can use equation (2) instead. However, we require a model that is able to calculate the cost driver rate of the activity as the sum of the cost driver rates of the tasks that constitute the activity. We use linear algebra to describe the theoretical basis of how our model does this here:

Let \mathbf{R} be a three-dimensional matrix that is used to record the capacity costs of each resource in each of the resource pools for a given task in an activity X. \mathbf{R} can be defined as such:

$$(7) \mathbf{R} = [r_{ijk}]_{u \times m \times p}$$

Where u = the number of resource pools, m = the maximum number of resources in any resource pool, p = the number of tasks in an activity and $1 \leq i \leq u$, $1 \leq j \leq m$, $1 \leq k \leq p$

Thus r_{ijk} represents the capacity cost rate of the j^{th} resource in the i^{th} resource pool when performing the k^{th} task of activity X. We then define the following vector with respect to activity X:

$$(8) \mathbf{t} = [t_i]_{1 \times n}$$

Where t_i represents the unit time of each task in \mathbf{R} and where $n = p$ for \mathbf{t} and \mathbf{R} , respectively.

Furthermore, we define the scalar v as the volume of activity X in a defined time period, such as a year. Bearing in mind the definition of cost driver rate as the product of capacity cost rate and unit time, the cost of activity X can then be derived using equation (2) as follows:

$$(9) \text{Cost of Activity X} = \text{Cost Driver Rate} \cdot \text{Volume}$$

$$= \left(\sum_{i=1}^u \sum_{j=1}^m \sum_{k=1}^p r_{ijk} t_k \right) \cdot v$$

TDABC and a Digital FORCFIPI – Information Query Simulation

In the event that X has variations, equation (9) can be applied separately to calculate the cost of each variation and the sum of the variations will yield the total cost of X and its variations.

To reiterate with respect to the model, the values that comprise \mathbf{R} and \mathbf{t} were defined in Excel, with v provided by SPSS and the total cost derived within Excel using equation (9).

In the following sub-sections we detail the results of the information query simulation.

8.2.3 Simulation: Information Query

In order to exercise the right to information privacy, as defined in Section 2.3.2, customers should be able to request the information about them that is stored by the organisation. In this scenario we simulated the activity of responding to an information query by a customer. The scenario took place in a large organisation that holds private information, mostly of a financial nature, about its customers. The activity consisted of a number of tasks that are discussed in broad terms below, and a subset of which are shown in Table 6 below.

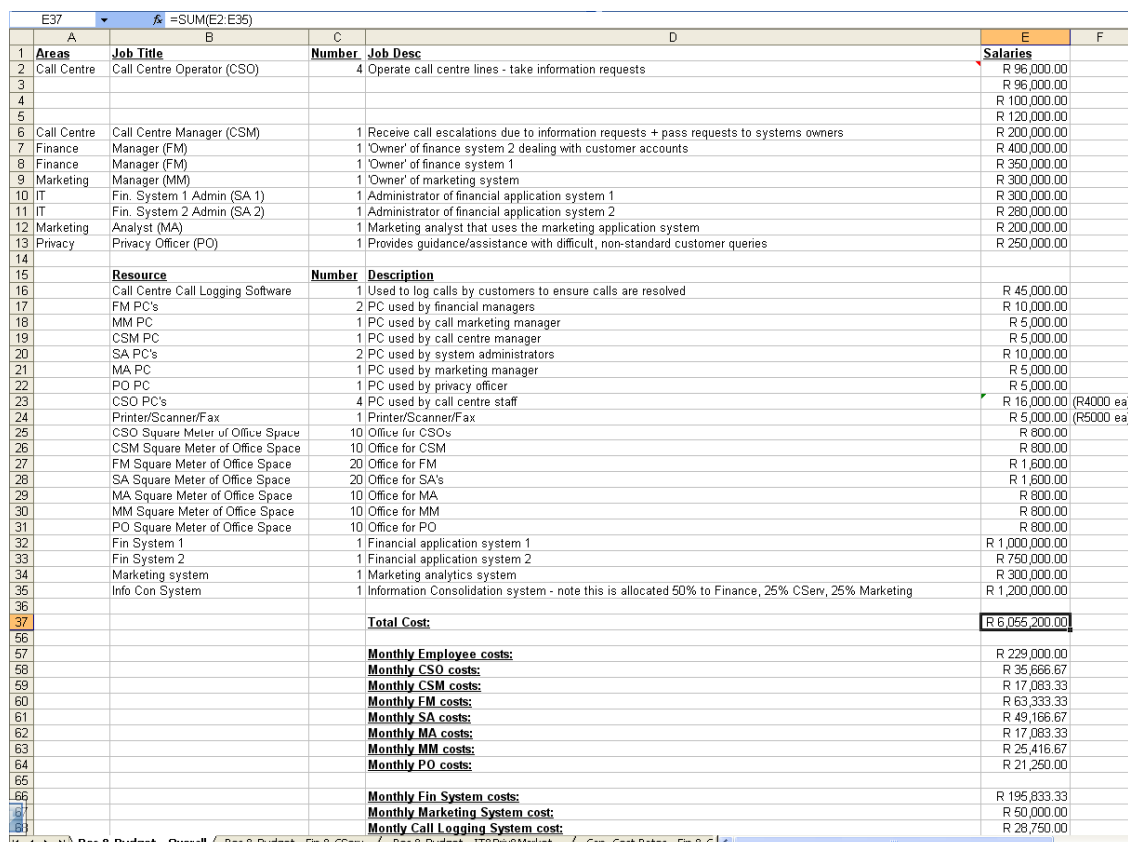
Our scenario involved a customer services department that ran a call centre for general enquiries by customers and the public. If a customer requested their personal information this would be handled first by a call centre operator (CSO). The request would then be handed to the customer services manager (CSM). The CSM would then make a request to the finance and marketing departments, who were responsible for the systems that contained customers' private information. The managers in the finance and marketing departments then requested their staff to access their systems for information on the customer in question. This information was subsequently approved by the finance managers (FMs) and marketing manager (MM) and returned to the CSM who compiled a report that was sent to the customer. If the CSM suspected a privacy violation may have occurred, such as the organisation having obtained or used the information inappropriately, the CSM consulted the information privacy team for instructions on how to proceed before getting back to the customer.

TDABC and a Digital FORCFIPI – Information Query Simulation

Table 6 – Subset of task times during an information query

Resource	Task	Level One (hrs)	Level Two (hrs)	Level Three (hrs)
CSO	Take call & authenticate customer	0.08	0.12	0.16
CSM	Take over call from CSO	0.08	0.12	0.16
CSM	Call up customer information	0.08	0.12	0.16
FM1	Approve request for information and facilitate release of information	0.08	0.12	0.16
MM	Approve request for information and facilitate release of information	0.08	0.12	0.16

The resources considered for the simulation included: salaries, the cost of PCs, two financial application systems, a marketing application system, call logging software for the call centre, printers and office rental. As mentioned in the previous section on the general TDABC model, the resource data, such as those of the information security team used in the scenario were entered into the TDABC model in Excel.



A	B	C	D	E	F
Areas	Job Title	Number	Job Desc	Salaries	
Call Centre	Call Centre Operator (CSO)	4	Operate call centre lines - take information requests	R 96,000.00	
				R 96,000.00	
				R 100,000.00	
				R 120,000.00	
Call Centre	Call Centre Manager (CSM)	1	Receive call escalations due to information requests + pass requests to systems owners	R 200,000.00	
Finance	Manager (FM)	1	'Owner' of finance system 2 dealing with customer accounts	R 400,000.00	
Finance	Manager (FM)	1	'Owner' of finance system 1	R 350,000.00	
Marketing	Manager (MM)	1	'Owner' of marketing system	R 300,000.00	
IT	Fin. System 1 Admin (SA 1)	1	Administrator of financial application system 1	R 300,000.00	
IT	Fin. System 2 Admin (SA 2)	1	Administrator of financial application system 2	R 280,000.00	
Marketing	Analyst (MA)	1	Marketing analyst that uses the marketing application system	R 200,000.00	
Privacy	Privacy Officer (PO)	1	Provides guidance/assistance with difficult, non-standard customer queries	R 250,000.00	
	Resource	Number	Description		
	Call Centre Call Logging Software	1	Used to log calls by customers to ensure calls are resolved	R 45,000.00	
	FM PC's	2	PC used by financial managers	R 10,000.00	
	MM PC	1	PC used by call marketing manager	R 5,000.00	
	CSM PC	1	PC used by call centre manager	R 5,000.00	
	SA PC's	2	PC used by system administrators	R 10,000.00	
	MA PC	1	PC used by marketing manager	R 5,000.00	
	PO PC	1	PC used by privacy officer	R 5,000.00	
	CSO PC's	4	PC used by call centre staff	R 16,000.00 (R4000 ea)	
	Printer/Scanner/Fax	1	Printer/Scanner/Fax	R 5,000.00 (R5000 ea)	
	CSO Square Meter of Office Space	10	Office for CSOs	R 800.00	
	CSM Square Meter of Office Space	10	Office for CSM	R 800.00	
	FM Square Meter of Office Space	20	Office for FM	R 1,600.00	
	SA Square Meter of Office Space	20	Office for SA's	R 1,600.00	
	MA Square Meter of Office Space	10	Office for MA	R 800.00	
	MM Square Meter of Office Space	10	Office for MM	R 800.00	
	PO Square Meter of Office Space	10	Office for PO	R 800.00	
	Fin System 1	1	Financial application system 1	R 1,000,000.00	
	Fin System 2	1	Financial application system 2	R 750,000.00	
	Marketing system	1	Marketing analytics system	R 300,000.00	
	Info Con System	1	Information Consolidation system - note this is allocated 50% to Finance, 25% CServ, 25% Marketing	R 1,200,000.00	
			Total Cost:	R 6,055,200.00	
			Monthly Employee costs:	R 229,000.00	
			Monthly CSO costs:	R 35,666.67	
			Monthly CSM costs:	R 17,083.33	
			Monthly FM costs:	R 63,333.33	
			Monthly SA costs:	R 49,166.67	
			Monthly MA costs:	R 17,083.33	
			Monthly MM costs:	R 25,416.67	
			Monthly PO costs:	R 21,250.00	
			Monthly Fin System costs:	R 195,833.33	
			Monthly Marketing System cost:	R 50,000.00	
			Monthly Call Logging System cost:	R 28,750.00	

Figure 20 – Screenshot showing resource data from TDABC model in Excel

TDABC and a Digital FORCFIPI – Information Query Simulation

A screenshot of this model is shown above in Figure 20. A detailed exposition of the resource costs can be found in Appendix C.

The information query activity had three variations that described the complexity required to fulfil the query. A Level One query was a straightforward query in which there were no complications in retrieving the customer information. A Level Two query was one which took longer, for example, a request for a customer record that had been archived in offline storage. A Level Three query was a more complex query that took longer than a Level Two query. Level Three queries would have included a request by a customer that wished to change or remove private information, or as part of complaint about an information privacy violation. The activities can be seen in more detail in Appendix D.

8.2.3.1 Statistics of the Simulation

The frequency of information queries was modelled as a uniform random variable between zero and an upper limit, l , specified as a parameter in the simulation. The probability, X , of an information query was then defined as follows:

- (10) $X \sim \text{Uniform}(0, l)$, where l = the maximum number of information queries in a month.

Of the non-zero queries, Bernoulli trials were used to determine the level of the information query. Each query had a 70% probability of being a Level One query, 20% probability of being a Level Two query and a 10% probability of being a Level Three query. The text box for “Max attacks/month” in the GUI for the simulation in Figure 21 below represents the simulation parameter l . The text box for “Number of months” represents the total number of months over which the simulation will be run.

TDABC and a Digital FORCFIPI – Information Query Simulation

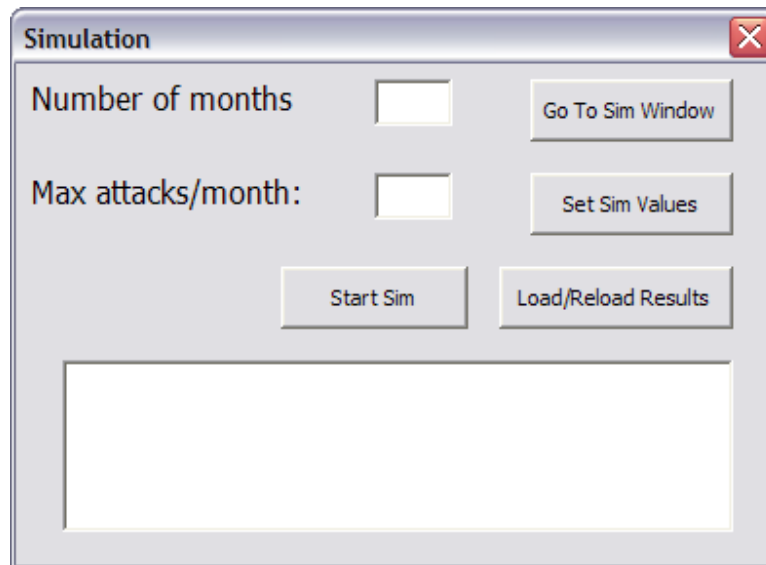


Figure 21 – VBA GUI used to enter simulation parameters for information query simulation

The code snippet of the SPSS Syntax used to produce the simulation results is shown below, with line numbers added for ease of reference. The probability of an event being a particular level is hard-coded into the SPSS Syntax between lines 12 to 20.

```

1 LOOP #Case = 1 to -99.
2 COMPUTE month = #Case.
3 COMPUTE #max_queries = -99.
4 COMPUTE #rand_queries = RV.UNIFORM(0,#max_queries).
  LOOP #i = 1 TO #max_queries.
5   IF (#rand_queries < #i) AND (#rand_queries >= #i -1) nr_queries = TRUNC (#rand_queries).
6   IF (#rand_queries = #max_queries) nr_queries = nr_queries-1.
7   END LOOP.
8   DO IF (nr_queries = 0).
9   COMPUTE criticality = 0.
10  END CASE.
11  ELSE IF (nr_queries > 0).
12  LOOP #j = 1 TO nr_queries.
13  COMPUTE #crit_level = RV.BERNOULLI(0.1).
14  IF (#crit_level = 1) criticality = 3.
15  DO IF (#crit_level = 0).
16  COMPUTE #crit_level = RV.BERNOULLI(0.7).
17  DO IF (#crit_level = 1).
18  COMPUTE criticality = 1.
19  ELSE IF (#crit_level = 0).
20  COMPUTE criticality = 2.
21  END IF.
22  END IF.
23  END CASE.
24  END LOOP.
25  END IF.
26  END LOOP.

```

TDABC and a Digital FORCFIPI – Information Query Simulation

Certain variables in SPSS Syntax are preceded by the '#' character. In the case of our simulation, the variable "#Case" defined in line 1 represents the number of months simulated. The variable "#rand_queries", defined in line 4, is a uniformly distributed real number between 0 and the user provided simulation parameter for the maximum number of queries a month. The maximum number of queries a month is the parameter l in equation (10) above and is represented in the code by the variable "#max_queries". "#rand_queries" is essentially the number of information queries in a given month. "#rand_queries" is however defined as a real number which may contain a fractional component. An integer is required since one cannot have a fraction of a query. The "TRUNC" function is used to obtain an integer, as shown in line 5. The result of the "TRUNC" function is stored in the variable "nr_queries" (line 5) which then represents the actual number of information queries in a given month.

In the code above, the variables "#Case" and "max_queries" are set to a value of -99. When the user inputs values for these simulation parameters in the Excel GUI, a VBA function replaces the values of -99 with the values input by the user. The simulation code is then self-explanatory when read with the explanation in the preceding paragraph.

The likelihood of the various query levels for each query and also for the number of queries per month were arrived at intuitively as we were unable to get empirical data on information queries at a large organisation. The lack of enforcement and consumer use of the PAIA meant that no organisation we approached kept such data.

It should be noted, though, that the simulation of the information queries was not designed to perfectly replicate a true, or 'real life', distribution of information queries since this was not the focus of our research. Rather, the simulation was designed to be a reasonable approximation of such queries. The primary aim of the simulation was to provide the TDABC model with a set of input data for the scenario in order to determine whether the model was useful for decision making by management. The ability of the TDABC model to function as a decision-making tool is of chief concern here rather than the specific input values being used in the scenario.

TDABC and a Digital FORCFIPI – Information Query Simulation

8.2.3.2 Simulation Results and Discussion

The results of a single simulation and experiment are presented here. A simulation was conducted to provide input to the TDABC model and the experiment conducted on the resultant TDABC model. The simulation simulated the yearly cost of responding to information queries. The simulation assumed a maximum of 40 information queries a month from customers, that is $l = 40$ in equation (10) above. Since X in equation 40 is a uniform random variable, larger values of l will result in greater values of X and therefore greater overall costs. 100 runs of the simulation were conducted and the average values were used as results. The simulation showed how TDABC can be used to determine the cost of responding to information queries. The specific costs determined by the TDABC model are displayed in Figure 22.

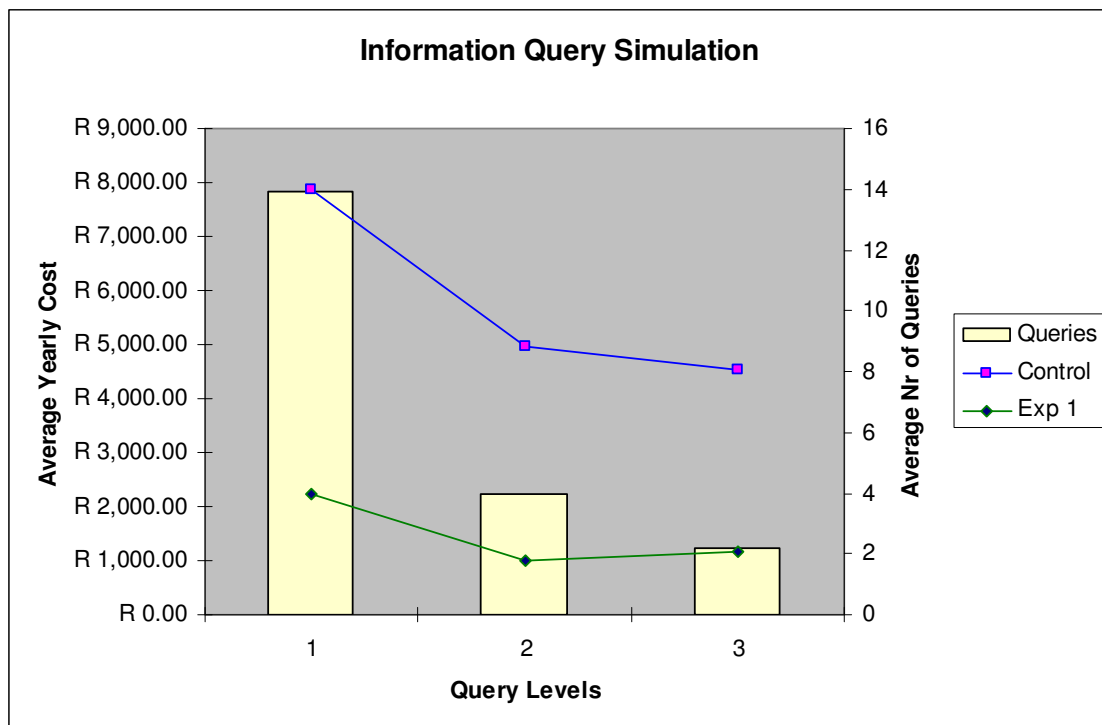


Figure 22 – Graph showing information query simulation results.

The bars in Figure 22, read against the right-hand Y-axis, show the average number of each type of query. The points on the lines, read against the left-hand Y-axis, indicate the average yearly cost associated with responding to each type of query. The ‘control’

TDABC and a Digital FORCFIPI – Information Query Simulation

simulation is marked as ‘Control’ and the experiment as ‘Exp 1’ in the legend. Level One queries caused the highest cost, followed by Level Two and Level Three queries.

An experiment was conducted to determine the impact of the purchase of an information aggregation or consolidation application for use by the customer services department. The purpose of the application was to consolidate customers’ private information from the various application systems, such as finance and marketing, into a single report for the CSM. The use of the application thus allowed for fewer tasks in the activity, especially from finance and marketing staff. This can be seen in Appendix E by the activity times in the table marked ‘-‘ that no longer need to be performed. The application also allowed more meaningful financial and marketing analysis and financial reporting. As such, 50% of the cost of the information consolidation application – R1.2 million – was allocated to the finance department and 25% to the marketing and customer services departments.

To conduct the experiment, the cost of the information aggregation application was added to the TDABC model and the appropriate tasks removed. The results showed cost reductions of 71.4%, 79.8% and 74% for Level One, Level Two and Level Three queries, respectively. Additionally, Level Three queries became marginally more costly than Level Two queries.

The experiment showed that TDABC can be used as a tool to forecast, and thus estimate, cost. In this instance a simulation was used as input to the TDABC model; however, an organisation may use historical data if such data is available. Together with the input data, only a small number of changes to the model were required to enable the cost to be forecast and the cost implications of the aggregation application understood.

The ability to estimate cost also allowed for a cost-benefit decision to be made. Here the forecast information from the TDABC model enabled the organisation to make a cost-benefit decision about acquiring the aggregation application – specifically, whether the cost savings resulting from the information aggregation application justify the cost incurred in purchasing it. Traditional cost systems would not be able to provide decision makers in the organisation with the cost-benefit of the purchase on each activity. It is

TDABC and a Digital FORCFIPI – Information Query Simulation

important to note that this also shows that TDABC can be useful to make cost-benefit decisions about the implementation of DFR measures.

A weakness of the simulation methodology used is that the fixed amount of time used for activities in the simulation, together with the fixed probabilities of different types of queries means that the results of the simulation may be derived analytically. In the next simulation we address this by making the amount of time used for an activity into a random variable. We also show an analytic technique for forecasting cost.

8.3 Conclusion

In this chapter we built on the discussion about managing costs in a digital FORCFIPI from the previous chapter. To show that TDABC can be used for cost decision making within a digital FORCFIPI we modelled a non-technical privacy-specific business process using a TDABC model. We then used a statistical simulation to provide input to the model and performed an experiment on the resultant model. The experiment together with the simulation showed that it is possible that TDABC can be used to inform management and used for implementation decisions in a digital FORCFIPI. In this case it was also shown that cost-benefit analysis and cost forecasts at the activity level were possible.

Due to a lack of comprehensive information privacy legislation and weak information access measures in South Africa at the time this work was undertaken, we were not able to test the use of TDABC and our digital FORCFIPI framework in a large organisation empirically.

The result is; however, still significant since, to our knowledge, this is the first work to propose the use of a cost management tool as means to manage and ascertain the costs associated with DFR. A digital FORCFIPI involves activities from the information security and information privacy functions of an organisation, thus the benefits of activity-level cost information accrue to these functions too. For this reason, we believe the result is relevant also to the field of information security management and the emerging field of information privacy management.

TDABC and a Digital FORCFIPI – Information Query Simulation

As mentioned in the discussion in the previous section, the simulation methodology described in this chapter did not involve any complex non-linear relations that would render expected values unreliable. Accordingly, in the next chapter we present a simulation that does contain non-linear relations, as well as an analytic cost forecast or projection technique. The simulation in the next chapter also differs as it is a simulation of a technical business process.

9 TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

9.1 Introduction

The simulation presented in the previous chapter was an example of how a TDABC model can be used together with a digital FORCFIPI. The simulation methodology used, however, meant that results similar to the simulation could be obtained analytically. In this chapter we show an analytic technique to obtain similar results. We also discuss another simulation that uses a methodology involving fewer linear relationships. It is therefore more difficult to predict the outcome of the simulation analytically. The simulation also uses an example of a technical business process, namely the monitoring of corporate firewalls.

A different simulation environment was used in the simulation presented in this chapter. This was due to the increased complexity of the simulation. While the simulation in the previous chapter consisted of approximately 30 lines of SPSS Syntax and 270 lines of VBA code, the simulation presented in this chapter comprised approximately 700 lines in the Java programming language (Java). The simulation environment and simulation results are also described in this chapter.

The rest of the chapter begins by describing an analytic technique that can be used to derive results similar to those arrived at by the type of simulation carried out in the previous chapter. The simulation environment, the statistics involved in the simulation and the results of the simulation then follow in order.

At the time of writing this thesis, the content of this chapter was accepted for publication in the journal *Information Systems Frontiers* (Reddy et al. 2011) and published “online first”. No further information on which volume and issue the article would be published in was provided by the journal, therefore the citation is to the Digital Object Identifier (DOI) provided by the journal.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

9.2 Analysis

The fact that TDABC is able to model activities through time equations means that it is particularly efficient at determining the cost of business processes which consist of a discrete number of steps. DFR processes typically are examples of such processes. Since cost is only a function of time, and time is captured in time equations that are simple linear equations, TDABC easily allows for “what-if” analyses to be conducted for different scenarios (Kaplan & Anderson 2007b, p.15). Such analyses are not possible using traditional cost systems and are significantly easier than in ABC since variations are more easily accommodated in the costing.

To show how a “what-if” analysis can be done, consider equation (4) for Total Activity Cost. The small alteration of moving c into the summation allows one to cater for different capacity cost rates. This is shown in equation (11) below. Equation (11) follows from equation (9) in the previous chapter.

$$(11) \text{ Total Activity Cost} = \sum_{i=1}^n c_i t_i v_i, \text{ where } n \text{ is the number of activities, } t \text{ the time to complete the } i^{\text{th}} \text{ activity, } v \text{ the volume of the } i^{\text{th}} \text{ activity and } c \text{ the capacity cost of the } i^{\text{th}} \text{ activity.}$$

Using this equation, managers can easily adjust the values for c_i , t_i or v_i to cater for different scenarios when budgeting. For example, they may consider the cost implication of hiring a new or an experienced employee. The difference in salary will be manifest in the value of c , while the estimated difference in time it takes a new versus an experienced graduate to complete a task can be modelled by adjusting the value of t . Kaplan and Anderson (2007b, p.15) note that such “what-if” analyses are carried out for budgeting purposes at the large, multi-national organisation Citigroup (Citigroup 2011). The simulation is discussed next.

9.3 Simulation

In this section we describe a simulation involving the combination of TDABC and the DFR-related business process of responding to firewall alarms. The technique of

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

simulation was chosen to demonstrate the use of TDABC with a DFR programme since the large organisations with DFR programmes in place in South Africa, typically banks, were not prepared to take part in a study for security reasons.

It should be noted, however, that the simulation was not designed to perfectly replicate a true, or ‘real life’, distribution of attacks on a corporate firewall since this was not the focus of our research. Rather, the simulation was designed to be a reasonable approximation of such attacks. The primary aim of the simulation was to provide the TDABC model with a set of input data for the scenario in order to show how the model can be useful for cost decision making by management. The assumption being that in a ‘real life’ scenario an organisation would be able to draw its own historical or current data to use as input for a TDABC model. The ability of the TDABC model to function as a decision-making tool is of chief concern here rather than the specific input values being used in the scenario. Below we discuss the simulation environment as well as the details and results of the simulation.

9.3.1 Simulation Environment

The simulation was conducted in Microsoft Windows XP using the Microsoft Office Excel 2003 spreadsheet (Excel) and the Java programming language (Java). As with the simulation in the previous chapter, the TDABC model for the simulation was developed in Excel. A Java program was then used to simulate attacks on a firewall and the response to such attacks by the relevant employees. The Stochastic Simulation in Java library (L’Ecuyer & Buist 2005)(Université de Montréal 2011) or SSJ, was used to generate random numbers. The JExcelAPI, or Java Excel API (JExcelAPI 2011), was used to produce output in the Excel file format, which allowed the TDABC model to incorporate the simulation results and update itself.

9.3.2 Firewall Alarm Simulation

In this scenario we simulated the response to firewall alarms by an information security team at a large organisation that holds private information, mostly of a financial nature, about its customers. The simulated scenario consisted of two information security officers (ISOs) and an information security manager (ISM) from the organisation’s

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

information security team. The ISOs were tasked with monitoring the firewalls and the ISM with managing the ISOs. The resources considered for the team included: salaries, the cost of PCs, two firewalls, printers and office rental. The detailed resources of the information security team used in the scenario can be seen in Appendix F. In addition, the scenario included the staff and similar resources from information privacy, finance and IT teams.

In the simulated scenario the activity of responding to firewall alarms was made up of numerous tasks. An example of the security team’s tasks in the activity and the respective expected times can be seen in Table 7. The activity also had three variations, namely Level One, Level Two and Level Three alarms. The choice of three levels is specific to our scenario – in a ‘real-life’ situation organisations will need to determine the number of levels according to their own circumstances and needs. A Level One alarm was defined as an alarm from the firewall in which, upon investigation, no breach of the firewall was detected.

Table 7 – Subset of task times during an information query

Resource	Task	Level 1 (hrs)	Level 2 (hrs)	Level 3 (hrs)
ISO	Investigate FW alarm	0.25	0.75	1
ISO	Write report of investigation to ISM	0.25	0.33	0.75
ISM	Analyse report & recommend action	0.17	0.33	0.75
ISO	Reconfigure firewall after recommendation	0.08	0.25	1
ISO	Draft monthly report item of incident	0.17	0.25	0.5

An example of a Level One alarm in our scenario would include repeated port scans from a single IP address. Level Two and Three alarms were deemed more serious and involved breaches of the firewalls. A Level Two alarm involved no access to the systems holding customers’ private financial information by an attacker, while a Level Three alarm involved access to such systems. In our scenario the organisation had chosen to apply DFR measures to monitor two financial applications that were deemed to be of greatest importance. The DFR measures modelled in the simulation were therefore

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

limited in scope to these applications. In certain cases, what may initially be thought to be a Level One or Level Two alarm may be upgraded to a higher level during investigation. In our scenario we also catered for these cases.

While Level One alarms were handled only by the security team, the other alarms involved the information privacy, finance and IT teams. The involvement by the other teams was primarily to determine the extent of the breach and what, if any, financial or private customer information was accessed or changed. Multi-disciplinary teams are further considered an important aspect of incident response (Yasinsac & Manzano 2001, p.292) to ensure that the broader interests of the organisation are better protected. In the DFR literature, it is also deemed best practice to pre-define the teams that will respond to an incident (Yasinsac & Manzano 2001, p.292)(Rowlingson 2004, p.21). This is in order to minimise any delay in response. As mentioned earlier, DFR processes should be focussed on systems on the basis of a cost-benefit analysis. Thus, it is possible to select teams that are relevant to the systems chosen in the cost-benefit analysis. Our scenario only includes the pre-defined teams and systems mentioned above. It is, of course, possible that any system may be compromised, however, our simulation is restricted to the above-mentioned systems. This is not unrealistic as budgetary constraints usually mean that only certain systems can be protected. Indeed, the reason TDABC is presented here is to enable the costing of DFR processes in order to better decide which systems will be protected and teams involved.

In the event of a zero-day attack, that is, an attack that exploits a previously unknown vulnerability in the firewall, we did not determine the cost. This was because, in our scenario, the response to a zero-day attack was to take the organisation offline until the vulnerability could be addressed. The cost of going offline is chiefly a function of the cost of conducting Internet-based operations manually, as specified in the organisation's business continuity plan. Determining this cost involved the complex task of modelling the organisation's Internet-based business operations and manual emergency operations. This level of complexity was beyond the scope of this scenario that sought to illustrate the general management of a firewall.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

9.3.2.1 Statistics of the Simulation

Modelling attacks on a firewall in the absence of historical data for a particular organisation is difficult. However, in the literature firewall and malware attacks have been modelled as Poisson processes (Tichenor 2007)(Greenfield & Tichenor 2009) and we follow the same approach here. The probability, X , of a successful attack was then defined as follows:

$$(12) X \sim \text{Poisson}(\lambda), \text{ where } \lambda = \text{number of successful attacks in a month}$$

The parameter λ was fixed for all the months in each run of the simulation. If an attack in a particular month was successful, a uniform random variable was used to determine the level of the alarm raised. A successful attack had a 73.5% probability of raising a Level One alarm, 14% probability of raising a Level Two alarm and a 12.5% probability of raising a Level Three alarm.

These values, though hypothetical, were based on the Computer Security Institute's 2009 Computer Crime and Security Survey (Peters 2009) results. The survey reported that 14% of respondents indicated a "system penetration by outsider" (Peters 2009, p.8). This corresponds directly with our definition of a Level Two alarm. The survey also cites financial fraud by 20% of respondents and unauthorised access by insiders at 15% (Peters 2009, p.8). Given the near even numbers of incidents of unauthorised access by insiders and outsiders, we make the assumption that half the incidents of financial fraud were at the hands of outsiders, i.e. 10%. Since a Level Three alarm involves access to financial systems this 10% forms part of the 12.5% likelihood for a Level Three alarm. Level Three alarms, however, also involve access to private information. In this regard, the survey reports unauthorised access to private information due to causes other than the theft/loss of a mobile device at 10%. We assume half of this unauthorised access (5%) occurs via a network. An assumption is again made that penetration by outsiders accounts for half of this, which results in 2.5%. Together with the 10% attributed to financial fraud this results in the figure of 12.5% for Level Three alarms. Level One alarms make up the remaining 73.5%.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

The reason for using the combination of survey results and assumptions rather than determining the values ourselves through empirical means was due to the unwillingness of the large organisations we approached to disclose such sensitive security information. As discussed earlier, though, the focus of our research was not to perfectly model a true distribution of attacks on a firewall. We instead aimed to provide a reasonable approximation of such attacks as input for the TDABC model. Given such input, which would be easier for an organisation to obtain in a real scenario, we then show that the TDABC model can be useful for costing and decision making by management. Again, the primary concern was that the TDABC model functions well as a decision-making tool rather than the specific input values being used in the scenario.

Once the level of an attack was determined, the amount of time taken by an employee to perform each task for that particular level was modelled as a random variable, Z , with an exponential distribution. The exponential distribution was chosen as it is typically used to model lifetime or the length of time of a process (Bain & Engelhardt 1992, p.115). It is a property of the exponential distribution that for it to have a mean x , the parameter of the distribution must be defined as x^{-1} . Z can therefore be defined with the following equation:

$$(13) Z \sim \text{Exponential}(t), \text{ where } t = \text{the inverse of the time taken to complete a task.}$$

An expected or ideal time was specified in the TDABC model for each task and these times, or values of t , were used as parameters for Z in each of the tasks. The decision to upgrade or escalate the level of an alarm was also determined by the value of Z . Where Z was greater than a single standard deviation from the mean, the level of an alarm was upgraded, for example, from Level 2 to Level 3. Costs were then calculated based on the times used for the upgraded alarm level.

The basic algorithm for the simulation can be seen in the following pseudo code:

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

FOR each month in the simulation:

Calculate number of successful attacks using Poisson distribution.

FOR each successful attack:

Determine level of alarm from uniform distribution.

FOR each alarm:

Look up expected task time for this level in TDABC model.

Create exponential distribution with expected task time as the distribution's mean.

Generate random time from distribution.

IF random time is greater than a single standard deviation from the distribution's mean,

upgrade the alarm to the next level and use expected times from the upgraded level.

Add time to output spreadsheet.

The simulation results are discussed next.

9.4 Simulation Results and Discussion

In our simulation, the time period of a month was the smallest time period simulated. In an initial simulation we simulated attacks on a firewall over 1200 months, or 100 years, with the parameter controlling successful attacks on the firewall, λ , equal to 2 (see equation (12)). Since there were a large number of time periods and the mean values for the probability distributions were given in the simulation parameters, the results predictably converged towards the specified mean values. The result can be seen in Figure 23 below. The bars in Figure 23, read against the right-hand Y-axis, show the average number of each type of alarm. The points on the lines, read against the left-hand Y-axis, indicate the average yearly cost associated with responding to each type of alarm.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

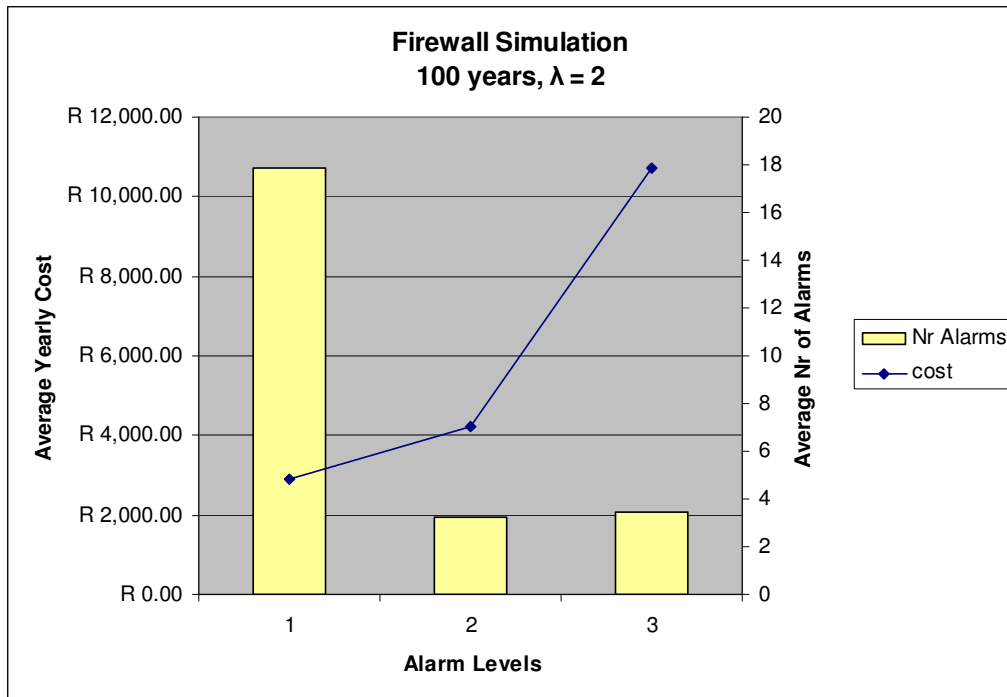


Figure 23 – Graph showing firewall simulation results over 100 years.

Since the values converged towards the specified mean values, these results are expected. The simulation, nevertheless, does show that TDABC can be used together with simulation to approximate the cost of responding to firewall alarms. Naturally, in a ‘real life’ scenario real data would be used to more correctly simulate the frequency of attacks and the distribution of each type of alarm. This simulation shows, though, that it is possible to provide input, simulated or not, to a TDABC model and have the model provide detailed cost information at the activity and even the task level – something that traditional costing methods cannot provide and that ABC cannot do as easily. Simulation, however, has the advantage of showing possibilities or scenarios that are not always as readily derived through analytic means. To illustrate this, we performed a series of 10 runs of a single year each with λ also equal to 2. These are shown in Figure 24 below.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

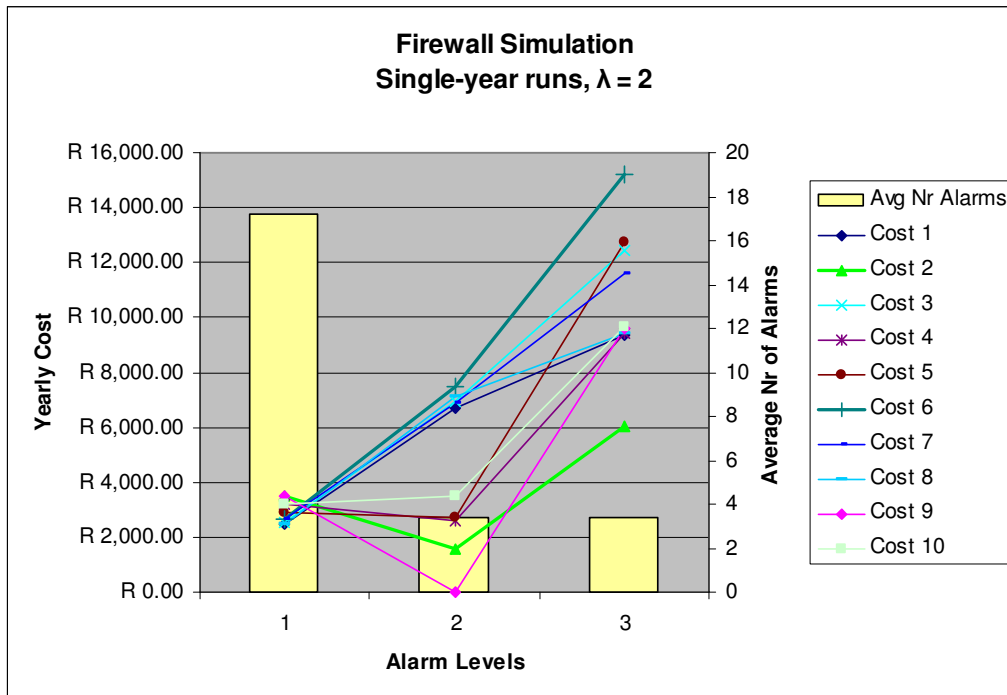


Figure 24 – Graph showing 10 simulation runs of a single-year each.

The graph in Figure 24 can be read similarly to the graph in Figure 23, with the exception that the bars represent the average number of alarms for the ten single years that were simulated. For readability, the lines referred to in the text are thickened. This type of simulation, where single years are simulated is more useful for decision making such as scenario planning than the previous, long-term simulation as depicted in Figure 23. The reason is that statistical variance has a greater impact over the short term than over the long term. For example, Figure 23 shows that over the long term Level 3 alarms cost an average of R10736. In Figure 24, Cost 6, or the cost in the 6th year simulated, shows that in a single year Level 3 alarms may cost as much as R15213 – 42% more. In a scenario planning exercise this may represent the worst case scenario for Level 3 alarms and allow management to take this under consideration when making cost versus risk decisions. Conversely, in the best case scenario in Cost 2, Level 3 alarms cost R6063 – 44% less than the average.

Figure 24 also shows that there are a number of years in which Level 2 alarms cost even less than Level 1 alarms, i.e. Cost 2 and Cost 9. This shows management that there may be years in which budget allocated to Level 2 alarms may be freed and used elsewhere.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

Another point that Figure 24 illustrates is the potential spread in terms of cost of Level 2 and Level 3 alarms. While the cost of Level 1 alarms in all the years seem to be clustered around a small range, Level 2 and Level 3 alarms show a different pattern. Almost half of Level 2 alarms are clustered between R6000 and R8000 and the other half between R0 and R4000. The reason for this is that because there is a higher volume of Level 1 attacks they converge towards the mean or expected value faster than Level 2 and Level 3 alarms. Although the explanation is reasonably straightforward, such a short-term spread in terms of cost may not be obvious to managers. This reiterates the point of simulation being useful in illustrating the statistical variance in the short term. Given the variance or spread in the cost of Level 2 and Level 3 alarms, management may wish to make changes to reduce the cost or risk. Next we show how the TDABC model can be used together with simulation to perform ‘what-if’ analyses.

We discuss the scenario where management considers purchasing firewalls to replace the two that are currently being used. The new firewalls cost double the price of the existing firewalls, yet promise to reduce attacks by up to 40%. To conduct a simple analytic ‘what-if’ analysis we doubled the cost of the firewalls in the TDABC model (as shown in Appendix F) from R75 000 to R150 000 each and observed the effect. Using the same data that produced the graph in Figure 23, we noted the effect to be minimal. The annual cost of responding to Level 1, 1, 2 and 3 alarms increased by 3%, 1% and 1%, respectively. To determine the potential effect of a 40% decrease in attacks on the firewall we simulated attacks over a 100 year period with λ equal to 1.2 instead of 2. Figure 25 below shows the results.

The simulation showed that in the long term the new firewalls would result in saving of 39%, 33% and 32% for Level 1, 1, 2 and 3 alarms, respectively. Firewalls are usually not used over a term as long as 100 years. Therefore, we also performed a series of 10 runs of a single year each to look at the potential short term effect of the new firewalls. This is shown in Figure 26 below.

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

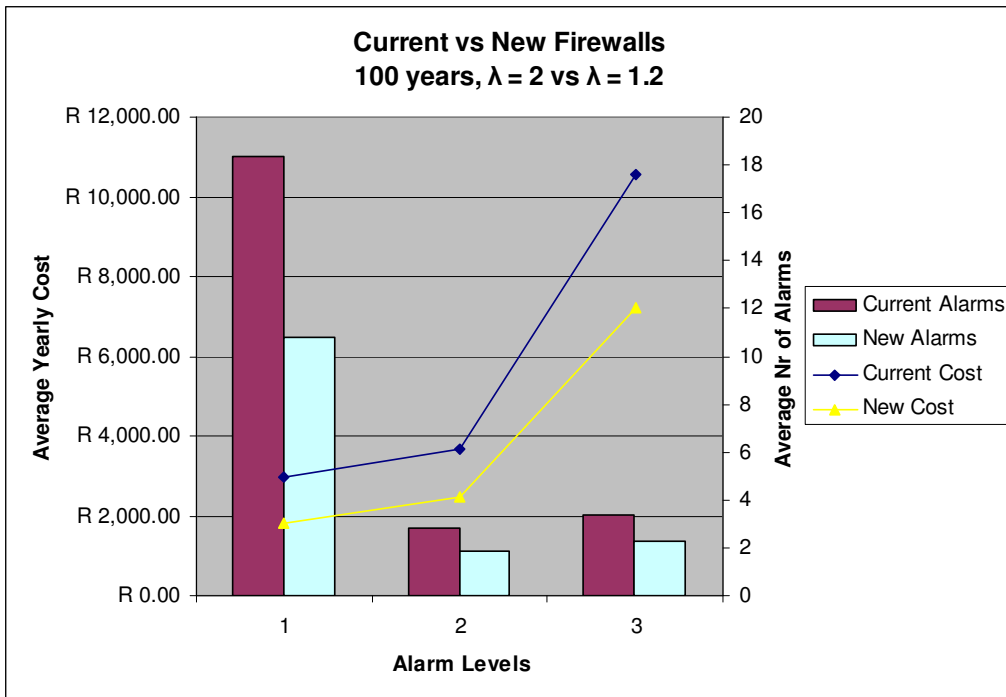


Figure 25 – Graph showing potential long-term effect of new firewalls.

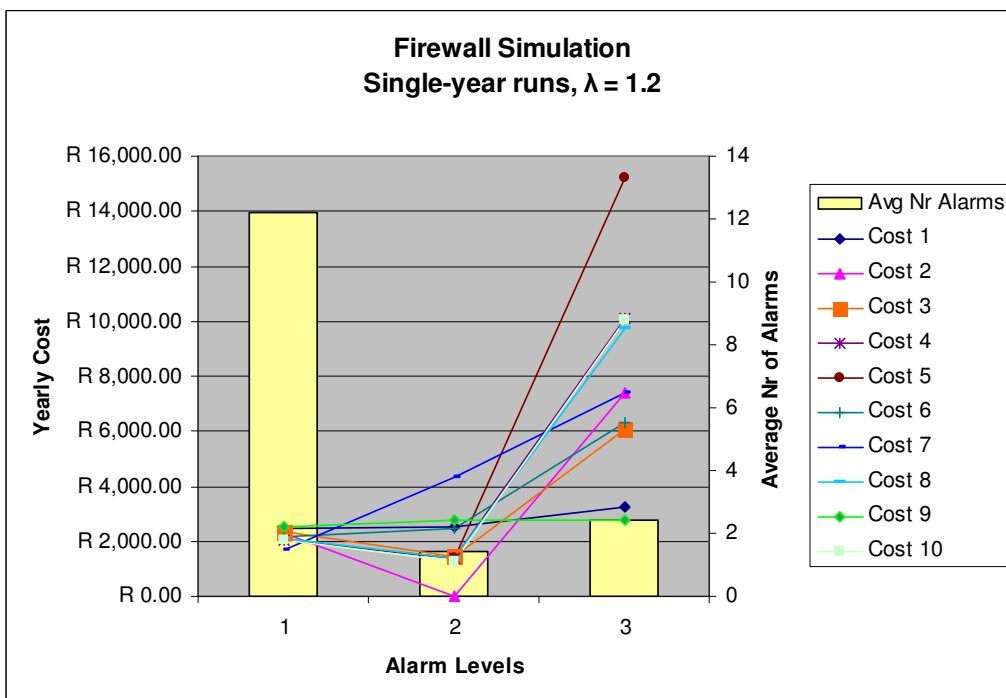


Figure 26 – Graph showing 10 simulation runs of a single-year each with new firewalls

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

The decision to purchase new firewalls needed to be based not only on a cost versus risk basis, but also on a cost-benefit basis, since there needed to be a justifiable benefit to replacing the existing firewalls. An important piece of information the simulation contributed to the risk decision can be seen when comparing Figure 25 with Figure 24 – the cost in the worst case scenario for a Level 3 attack is almost the same in both graphs. This meant that if the classic definition of risk as the product of likelihood and impact (Bahli & Rivard 2005, p.176) was used, the impact remained the same while the likelihood decreased.

The simulation also contributed with regard to the cost-benefit decision. The simulation was able to show that in the short term, the new firewalls may be able to lower the average cost of Level 1, 1, 2 and 3 alarms by 25%, 59% and 26%, respectively. Of course, the installation of new firewalls may have impacted other activities and business processes, either by increasing or decreasing cost. In the scenario, management needed to determine whether such a potential impact over the short term justified the expense. Next, we look at some of the limitations of our simulation.

In the discussion thus far, the accuracy of the values produced by the simulation is dependent on the accuracy of the assumptions made in the design of the simulation. We have identified the following limitations in the simulation:

- **The frequency and distribution of attacks.** As mentioned, the values for the frequency of successful attacks are based on reasonable estimates from survey results and not directly on empirical data for any particular organisation. While we cannot guarantee the realism of the values provided, we argue that in a real scenario the accuracy of a simulation can be increased by using empirically derived data.
- **Modelling of activity times.** The times taken to complete tasks were, for the most part, modelled as independent random variables. This is not entirely accurate as an unusual case that takes the security team more time to respond to, may also take the other teams a longer time to respond to. We made this assumption as the alternative implied the use of multivariate random distributions to model the activity times, which we felt was overly complex for the purpose of

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

our simulation, namely to provide input for the TDABC model. In the case of upgrading the level of an alarm, the task times were not independent since the upgrade was a function of the time taken.

We conclude the chapter in the next section.

9.5 Conclusion

In this chapter we showed how TDABC is useful in determining costs by briefly presenting a simple analytic technique that can be used with a TDABC model to perform ‘what-if’ analyses for budgeting and other decision making. We then used a statistical simulation to provide input to a TDABC model. As with the simulation presented in the previous chapter, we showed that information from the simulation and TDABC model could be used for decision making. The analysis showed how TDABC can be used for cost forecasting in a digital FORCFIPI. The simulation showed that it is possible for TDABC to be used for decision-making in a digital FORCFIPI, specifically for cost-benefit decisions.

The technique of simulation was also shown to provide management with cost information regarding potential short and long-term scenarios – information that is useful in decision making. Lastly, the simulation methodology used in this chapter was an improvement over the methodology used in the previous chapter because it could not be replicated by straight forward analytic techniques. The simulation methodology presented in this chapter should be used in situations where non-linear relations exist in the process being simulated. That is, where the outcome of a random variable being modelled is a function of another random variable. Where random variables are used that do not depend on the value of other random variables, the simulation methodology in the previous chapter can be used. A comparison of the two simulations can be found in table form in Appendix H. The simulation presented in this chapter did, however, have certain limitations, which were outlined in the chapter.

In the next chapter we discuss an architecture for a DFR management system (DFRMS) that can assist in the management of DFR, including DFR for information privacy

TDABC and a Digital FORCFIPI – Firewall Monitoring Simulation

incidents. The DFRMS architecture assists in the practicalities of managing DFR and takes the management of cost into account as well.

10 Architecture of a Digital Forensic Readiness Management System

10.1 Introduction

In the preceding chapters we discussed a framework and costing methodology that can be used to help a large organisation follow a coordinated, risk-based approach to managing DFR, specifically with regard to a digital FORCFIPI. In this chapter we help address the challenge of managing the DFR function within a large organisation by proposing an architecture for a digital forensic readiness management system (DFRMS). Besides assisting in the management of DFR in general, a DFRMS can also help with the management of a FORCFIPI. A detailed discussion on how it is possible to do this is presented in the next chapter in Section 11.4. A costing methodology such as TDABC, when applied to DFR, can also be implemented through a DFRMS. This is possible by automating the calculation of TDABC-derived costs in a DFRMS. While there are a number of software tools and systems within the domain of digital forensics, our review of the literature did not reveal a system dedicated to assisting the management of DFR. The DFRMS architecture proposed here is, therefore, novel. The specifications for the DFRMS are drawn from a requirements analysis undertaken by surveying the literature on DFR. The results of this requirements analysis are also presented in this chapter. Before the requirements analysis is presented, however, we look at related work, which follows in the next section. The requirements analysis follows immediately after the section on related work and the architecture is presented subsequently.

10.2 Related Work

As mentioned, our review of the literature did not reveal any software or tools dedicated to the management of digital forensic readiness (DFR). In this section we therefore discuss software or tools that are related to, but are not dedicated to, the management of DFR. Digital forensic analysis tools, which are used for analysis during investigations, are not discussed. For example, Raghavan et al. (2009) presented an open forensic integration architecture for digital evidence; however, this is focused on the analysis phase of the digital forensic process.

Architecture of a Digital Forensic Readiness Management System

Three types of software were identified that are directly related to the management of DFR, these are: intrusion detection systems, security event management software and incident management software. A discussion of each type follows.

10.2.1 Intrusion Detection Systems

Intrusion detection systems (IDSs) are related to the management of DFR because they enable the monitoring of events on computers and networks. It has been shown in Section 4.2.1, the monitoring of events is required for DFR. Gengler (2002, p.4) defines intrusion detection as “the process of monitoring the events occurring in a computer system or network and analysing them for signs of intrusion”. She in turn defines an intrusion detection system (IDS) as a software or hardware system that automates the intrusion detection process. IDSs typically collect data from networks, applications, or hosts on a network. The data from networks is primarily network traffic, while application data is in the form of application logs or events. Finally, host data usually takes the form of operating system logs (Venter 2002, p.29-30). IDSs analyse the data to determine if an intrusion has occurred. If so, the IDS raises an alarm and/or sends a notification to the appropriate individuals.

Next, we look at security event managers.

10.2.2 Security Event Managers

Security event managers (SEMs), security information managers (SIMs) and security information and event managers (SIEMs) are all names given to security event management software or appliances. The names are synonymous and the software or appliances typically perform the same function regardless of name (Swift 2007, p.3-4). For the sake of consistency we use the term security event managers (SEMs). SEMs were developed as a result of the inability of IDSs to effectively filter real threats from false alarms and normal system activity (Mehdizadeh, 2005, p.18). Although relatively new, SEMs constitute one of the fastest growing segments of the information security technology market (Deloitte 2010, p.4).

Architecture of a Digital Forensic Readiness Management System

SEMs are related to the management of DFR since, like IDSs, they also monitor events or data from multiple sources. SEMs, however, usually perform additional tasks. Swift (2007, p.4) lists four important functions that all SEMs perform:

- **Log Consolidation.** Centralised logging to a server is used to consolidate logs.
- **Threat Correlation.** Artificial intelligence techniques are applied to sort through multiple logs and log entries in order to identify attackers or threats.
- **Incident Management.** Workflows are defined and stored to determine what happens once a threat is identified. This is the path from the initial identification of a threat to the threat's containment and/or eradication. Incident management includes: notification; trouble ticket creation; automated responses, such as the execution of scripts; and lastly, response and remediation logging.
- **Reporting.** Reports on operational efficiency and effectiveness can be produced, as well as reports tailored for regulatory compliance, and reports that may be needed for ad-hoc enquiries and forensic investigations.

IDSs are different to SEMs as they do not typically perform all of the tasks listed by Swift above, moreover, SEMs may in fact make use of IDSs to perform their functions (Mehdizadeh 2005, p.21). We reviewed the product websites of ten SEMs and determined that some additional features are advertised by SEM manufacturers. Some of the additional features are presented in Table 8. A 'Y' in Table 8 indicates that the product has a particular feature, while an 'N' means it does not. An 'S' indicates that the product has some but not all the functionality associated with the feature.

In Table 8, all SEMs have a data analysis capability. Data analysis refers to the ability to perform arbitrary queries or analysis of consolidated log data. All of the SEMs also encrypted or digitally signed stored event data. This is to prevent tampering with the event data. File integrity monitoring was a feature that appeared in three SEMs. File integrity monitoring allows SEMs to monitor when specific files are changed, viewed or deleted. Many SEMs also support the ability to monitor the actions of specific users on operating systems or networks. User monitoring was supported in five of the sampled SEMs while two supported limited user monitoring. Only two SEMs supported geolocation functionality. Geolocation allows SEMs to display the geographic location

Architecture of a Digital Forensic Readiness Management System

of attacks for organisations that are dispersed over a wide geographic area. The SEMs claim to also show the geographic source of an attack. Lastly, four SEMs fully supported the ability to determine whether the configurations of devices or hosts on a network had changed – a feature known as device configuration audit. Two of the SEMs advertised limited device audit configuration features.

Table 8 – Additional features found in SEMs currently in the market.

Product / Feature	1	2	3	4	5	6	7	8	9	10
Data analysis	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Hashed / encrypted event storage	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
File integrity monitoring	N	N	Y	N	N	N	Y	N	N	Y
User activity monitoring	N	N	Y	N	S	Y	Y	Y	Y	S
Geolocation	N	N	Y	N	N	Y	N	N	N	N
Device configuration audit	Y	N	Y	N	S	Y	S	N	S	Y

The next category of related work is incident management software.

10.2.3 Incident Management Software

Within the context of information security (IS), an incident can be defined as: an identified occurrence of a system, service or network state indicating a possible breach of IS policy or failure of safeguards, or a previously unknown situation that may be relevant to security (Kostina et al. 2009, p.94). In large organisations incidents are usually reported to a central point, normally a help desk or service desk (Gupta et al. 2008, p.141). Incident management software assists the organisation by facilitating the incident management process, which consists of, *inter alia*, incident detection, classification, analysis/diagnosis and finally repair and recovery (Gupta et al. 2008, p.142)(Metzger et al. 2011, p.114). Incident management software assists by controlling the workflow involved in the incident management process. In order to do this the software also contains “incident records, escalation rules, information about customers and end users, and information about configuration items” (Jäntti 2009, p.184).

Architecture of a Digital Forensic Readiness Management System

Both SEMs and incident management software control some or all of the workflow in the incident management process and there is therefore an overlap of functionality between the two. SEMs, however, only deal with IS incidents while most dedicated incident management software deals with IT incidents in general. It is of course up to organisations to determine if they prefer to deal with IS incidents separately or if they prefer a more unified approach.

In the next section, we examine the requirements for a DFRMS.

10.3 Requirements Analysis

In order to determine the requirements of a DFRMS we examined the literature on DFR. As mentioned in Section 4, perhaps the single greatest contribution to the concept of DFR has been that of Rowlingson (2004). A number of requirements therefore stem from Rowlingson's work. In this section we discuss each of the requirements garnered from these and other authors. The requirements are discussed below under the headings of 'monitoring', 'DFR information' and 'cost'. The requirements are also summarised in Table 9 below.

10.3.1 Monitoring

Among the contributions of Tan's initial work is the identification of the importance of logging network and host activity in an organisation. To be ready to perform a DF investigation it is first necessary to have a record of network activity or the actions performed on a host. A DFRMS should therefore have a monitoring component capable of monitoring and logging the activity within an organisation's IT infrastructure. It follows, thus, that a DFRMS must have the ability to receive events from a range of hardware and software platforms and store them securely. Tan (2001, p.3) makes specific mention of IDSs – we believe the reason for this is that IDSs were the state of the art in monitoring technology at the time. The secure storage of log data is necessary to preserve its value as evidence. If logs are open to be edited their value as evidence is diminished since they cannot be relied on as much to be accurate. To this end, log data

Architecture of a Digital Forensic Readiness Management System

should not only be kept in a secure manner, but also digitally signed or encrypted to prevent tampering (Tan 2001, p.20).

Any system that performs monitoring must also be able to represent the elements being monitored. For example, it should be possible for a user to choose an element being monitored and know from the DFRMS that the element is a firewall. A monitoring capability also requires that a DFRMS should be able to distinguish multiple events from each element being monitored. Using the example of the firewall again, a DFRMS should be able to distinguish that a firewall is signalling a port scan as opposed to a flooding attack.

The detection of events that constitute a potential or actual incident should be automated and an alarm raised whenever the events are detected (Grobler et al. 2010, p.678). Monitoring, however, is only a single dimension within DFR. We now look at other requirements, which we discuss collectively under the title 'DFR information'.

10.3.2 DFR Information

As with incident management software that stores escalation rules and configuration information, a DFRMS also needs to store current information required for the purposes of DFR. This information is information that can be used predominantly in two cases: firstly, by the DF personnel that conduct investigations; or secondly, by employees that are required to respond to incidents. Examples of such information are, in the first case, a procedure on how to retrieve information from a desktop computer, and, in the second case, an escalation procedure when suspicious activity is noted. The information also pertains to the operations of the DF function, for example, information on the DF training of DF personnel.

The importance of monitoring and logging has been mentioned above, however, it is important that hardware and software is first configured to log activity adequately (Casey 2005, p.259). A DFRMS must therefore contain the necessary configuration procedures and standards for the IT, IT security, information privacy and DF staff that may be responsible for configuring hardware and software.

Architecture of a Digital Forensic Readiness Management System

In this thesis, and indeed in the architecture, we differentiate between incident response and DF teams. We define incident response teams as those individuals that respond the instant an incident is detected. They may be from departments completely outside of DF, such as IT. A system administrator whose job it is to stop a process executing on an operating system in response to an incident is an example of an incident response team member. In contrast, we define DF teams as consisting of individuals with specialised DF skills involved in the investigation of incidents. Yasinsac and Manzano (2001, p.292) as well as Lamis (2010, p.177) note that DF teams and incident response teams should both be defined *a priori*, that is, in anticipation of an incident and not after an incident occurs. If this is not done, valuable time and evidence may be lost while teams are constituted. Thus, it should be possible to define and then store such teams in a DFRMS for easy accessibility and for automated notification should incidents occur. Yasinsac and Manzano (2001, p.292) as well as Chen et al. (2005, p.6) and Rowlingson (2005, p.10) also discuss the importance of training the incident response and DF teams. Training is important as untrained staff may compromise or lose evidence through their actions. In light of this, we believe a DFRMS should have the capacity to record the training undertaken by team members. This will allow managers to determine if teams contain the requisite skills.

According to Rowlingson (2005, p.5) in order to take a risk-based approach to DFR it is vital to “define the business scenarios that require digital evidence”. Hence, a DFRMS should be able to store descriptions of the business processes that DF is involved in. If the business process descriptions are kept up to date, perhaps through a formal system of updates, then DFR management is in a position to react to changes in business processes that may increase risk. The increased risk referred to is 1) the business risk DFR operations were put in place to mitigate; or 2) a risk to the effectiveness of DFR operations themselves.

Organisational policy, such as an overall forensics policy, should form the basis for DFR (Yasinsac & Manzano 2001, p.292)(Rowlingson 2005, p.8)(Taylor et al. 2007). Thus, the staff involved with DFR should have access to the necessary policies to inform their decision making. The policies contemplated here include, *inter alia*, the policies in

Architecture of a Digital Forensic Readiness Management System

Levels A and B of the digital FORCFIPI (see Section 6.3.1) and the business policies in block F6 (see Section 6.3.3). A DFRMS system will therefore need to store policies that are relevant to DFR. Besides an overall organisational policy, Rowlingson (2005, p.9) advocates a suspicion policy that can be used by monitoring staff to determine what constitutes suspicious behaviour in the infrastructure being monitored. The suspicion policy should also be included in a DFRMS. The nature of some incidents requires that they be reported to law enforcement for legal or ethical reasons (Lamis 2010, p.182), for example, child pornography found on an employee's computer. A policy offering guidance on when to contact law enforcement should exist (Danielsson & Tjøstheim 2004, p.420) and must be stored on a DFRMS.

A suspicion policy that defines suspicious behaviour would ideally also be associated with an escalation procedure document that guides individuals on: how to escalate suspicious behaviour, for example via telephone or email; and, who to escalate it to, for example the IT Security Manager (Yasinsac & Manzano 2001, p.292)(Rowlingson 2005, p.9). An escalation procedure document should therefore also be included in a DFRMS. If suspicious behaviour proceeds to be an incident, or once an incident is discovered, an incident response procedure is required (Casey 2005, p.259)(Chen et al. 2005, p.4)(Rowlingson 2005, p.9). The incident response procedure details the steps that must be followed for different types of incidents and is hence required in a DFRMS. If law enforcement needs to be contacted per the law enforcement contact policy mentioned earlier, a specific law enforcement contact and handover procedure should exist. This procedure should be available on the DFRMS and detail report formats etc. (Danielsson & Tjøstheim 2004, p.420).

It is most probable that in the policies and procedures mentioned above reference will be made to staff positions in the hierarchy of an organisation. For example, it may be policy to notify the Chief Forensics Officer for incidents deemed to be of the highest severity. Likewise, the definition of DF teams and incident response teams discussed above may also refer to staff positions in the hierarchy of an organisation. Indeed, as mentioned in Section 3.2.1.2, Beebe and Clark (2004, p.4) state that a response to an incident should be a coordinated effort amongst “managerial, human, legal, and law enforcement resources”.

Architecture of a Digital Forensic Readiness Management System

The organisational hierarchy, together with contact details for all staff included in the hierarchy, should hence be stored in a DFRMS to enable the correct staff to be contacted as soon as possible.

As previously mentioned, the requirements that have been discussed are summarised in Table 9 below. In the sub-section that follows we discuss cost.

Table 9 – DFRMS requirements from the literature

Requirement	Citation / Reason
1. Monitor or log network and host activity	Tan (2001, p.2)
2. Secure storage of logs	Tan (2001, p.20)
3. Intrusion detection system	Tan (2001, p.3)
4. Distinguish between hardware or software elements being monitored	Follows from requirement 1
5. Automated alarm upon detection of potential or actual incident	Grobler et al. (2010, p.678) and also follows from requirement 3
6. Configuration procedures for monitoring and logging	Casey (2005, p.259) and follows from requirement 1
7. Investigative teams (DF teams) and incident response teams descriptions	Yasinsac and Manzano (2001, p.292)
8. Training requirements and training received	Yasinsac and Manzano (2001, p.292), Chen et al. (2005, p.6), (Rowlingson 2005, p.10)
9. Business process descriptions	Rowlingson (2005, p.5)
10. Organisational DF policies organisational and policies related to DFR	Yasinsac and Manzano (2001, p.292), Rowlingson (2005, p.8), Taylor et al. (2007).
11. Suspicion policy	Rowlingson (2005, p.9)
12. Law enforcement contact policy	Danielsson and Tjøstheim (2004, p.420), Lamis (2010, p.182)
13. Escalation procedure	Yasinsac and Manzano (2001, p.292), Rowlingson (2005, p.9)
14. Incident response procedure	Casey (2005, p.259), Chen et al. (2005, p.4), Rowlingson (2005, p.9)
15. Law enforcement contact procedure	Danielsson and Tjøstheim (2004, p.420)
16. Organisational structure and staff involved in DFR and incident response	Follows from requirements 7, 8, 10, 11, 12, 13, 14, 15

10.3.3 Cost

As mentioned in mentioned in Chapter 7, cost is an important aspect of DFR since DF management typically works with a limited budget. Budget should be spent relative to risk. That is, the first priority when spending budget should be the risks that are 1) greatest in terms of potential loss, and 2) mitigated the most through the use of digital

Architecture of a Digital Forensic Readiness Management System

evidence (Rowlingson 2005, p.5). A DFRMS should therefore be able to assist in determining the cost of DFR measures so that these costs can be weighed against the potential loss associated with a particular risk. In this regard, the DFRMS should implement TDABC or some other mechanism for determining costs.

10.4A DFRMS Architecture

In this section we present an architecture for a DFRMS. The overall architecture is presented briefly now and is followed by a more detailed exposition of the constituent components of the architecture in the sub-sections that follow.

The term ‘architecture’ is a widely used term with different meanings in different contexts. There is also considerable disagreement over the definition of the term (Baragry & Reed 2001). Therefore, before presenting the architecture, we define the term as it relates to the architecture presented here. We adapt the definition of an architecture used in TOGAF (Open Group, 2012), which is a widely used standard for enterprise architecture from the Open Group (Open Group, 2006). We define an architecture as follows:

A description of a system, the structure of its components, their inter-relationships, and the principles and guidelines governing their design and implementation.

This definition means that our architecture is at a higher or more conceptual level than a traditional software architecture. Traditional software architectures fall into the following classes as defined by Baragry and Reed (2001, p.131): Static Implementation Architectures and Dynamic Operation/Execution Architectures. These offer more detailed descriptions of the design and implementation of the individual components in our architecture. We do not discuss the components at this level of detail.

At the highest level the architecture consists primarily of five modules, namely: the event analysis module, DFR information management module, costing module, access control module and user interface module. The modules are so called since a modular architecture is proposed in which the modules are able to function relatively independently from one another. The event analysis module, DFR information

Architecture of a Digital Forensic Readiness Management System

management module and costing module aim to meet the monitoring, DFR information and cost requirements mentioned in the previous section. The access control module, as its name suggests, handles access control for the system and is coupled with the user interface module since access rights determine what is available in the user interface. Figure 27 shows a high-level view of the architecture.

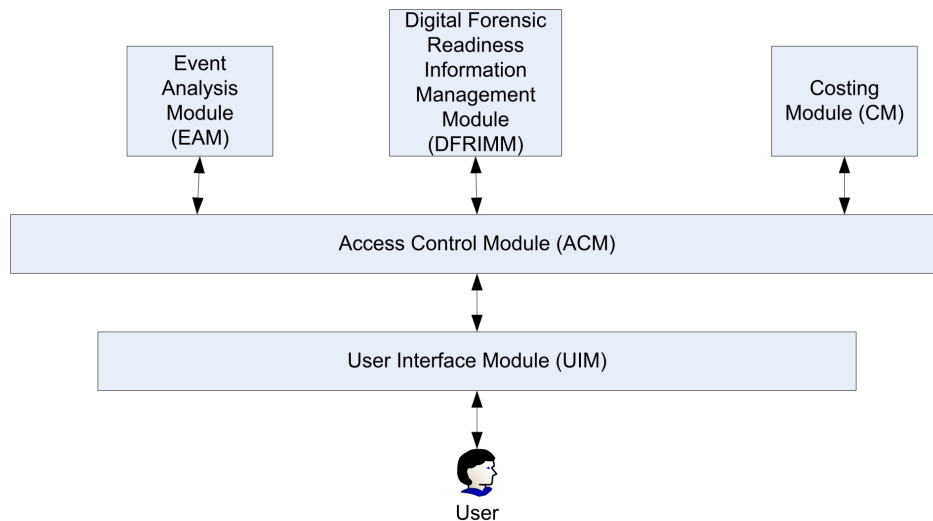


Figure 27 – High-level view of the architecture

10.4.1 Event Analysis Module

The event analysis module (EAM) receives events from hardware and software entities in the IT infrastructure. The components that make up the EAM can be seen in Figure 28. The databases shown in Figure 28 are not necessarily multiple databases, but are shown as such for illustrative purposes – that is, they are a logical representation, but not necessarily a physical representation. In Figure 28 double-sided arrows indicate two-way communication between components. Single-sided arrows signify one-way communication from the component to the arrow's target. Dashed lines indicate queries where information is requested from databases.

The EAM alerts users based on pre-defined alert definitions. Users with sufficient privileges can create alert definitions that are comprised of a single event or a combination of events. Alert definitions are typically created to indicate suspicious activity or activities that are of interest to DF staff. Alert definitions, once created by

Architecture of a Digital Forensic Readiness Management System

users, are stored in encrypted form in a database. Encryption is used so that if the database is compromised there is no disclosure of the activities being monitored.

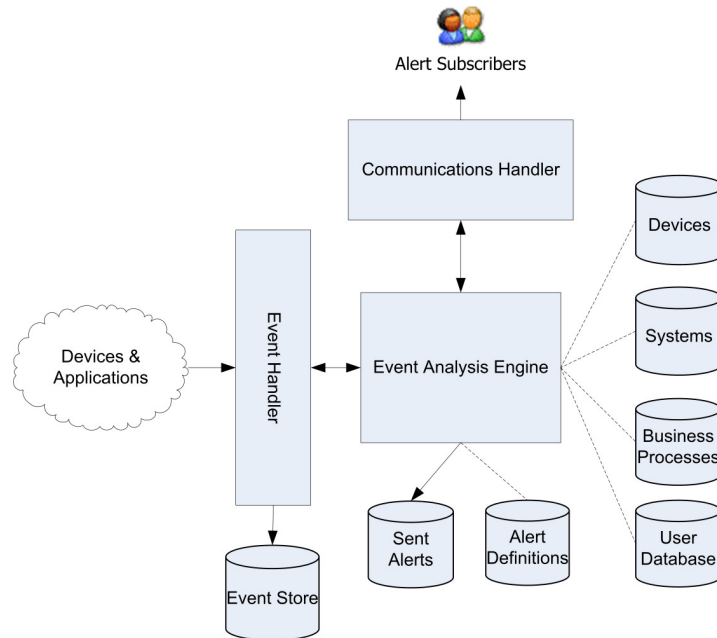


Figure 28 – Figure illustrating components of the Event Analysis Module.

Alerts are defined with respect to one or more of the following: devices, systems and business processes. A device is typically hardware, for example, a router or firewall. System refers to software, such as an application system or the operating system on which the application system resides. Lastly, business process refers to the definition of a business process by Hammer and Champy cited in Lindsay et al. (2003, p.1015), namely: a set of partially ordered activities intended to reach a goal. Alerts are only possible for business processes that make use of devices or systems. In such cases, in the definition of the business process, a device or system will be associated with the business process. When any of the devices or systems that have been associated with the business process trigger an alert, the business process alert will also be triggered. The reason for defining alerts with respect to business processes is that certain business processes, for example, the accounts payable business process, have a higher risk associated with them. In these instances management associated with the business process may need to be notified regarding events that signify potential danger. In order to receive alerts, users must subscribe to alerts, or they must be subscribed to alerts by certain high-level users who

Architecture of a Digital Forensic Readiness Management System

are allowed to subscribe other users, such as managers. The databases that store the devices, systems and business processes are shown using database symbols, which are the symbols on the extreme right of Figure 28.

In the architecture we do not mandate a particular approach to event analysis, such as a straight forward rule-based approach, or an approach based on some form of artificial intelligence (AI). The choice of analysis technique is left as a design choice. The analysis of rules or the execution of AI is performed by the event analysis engine (EAE).

In practice dealing with events from hardware or software entities is not trivial for two reasons. Firstly, not all hardware and software entities are designed to explicitly provide event information (Karlzén 2009, p.12). Secondly, where hardware and software entities have been designed to explicitly provide event information, the event information may be formatted according to a number of different standards (Karlzén 2009, p.12)(Swift 2006, p.16). In order to resolve the first problem, it is necessary for the DFRMS to use techniques that are similar to those used by SEMs. SEMs make use of software known as event collectors, or agents, to extract event information from hardware or software entities that do not explicitly provide event information (Nicolett 2008, p.2). In the DFRMS, event collectors or agents must also be used to send event information to the EAM in an appropriate format. To solve the second problem, the DFRMS should cater for all the necessary event information standards that are used by hardware and software entities in a particular organisation.

The EAE does not receive events directly from hardware or software entities. It receives events from a separate event handler which receives communication directly from hardware and software. The event handler serves as an intermediary in order to abstract the communication function from the analysis function.

Besides monitoring and alerting, a primary function of the EAM is to log events. To this end, the event handler does not only pass events to the EAE, but stores all events directly in a database in encrypted form. The reason the event handler also stores events directly in the database is twofold. Firstly, if events are passed via the EAE to the database and not directly, a failure in the EAE would result in lost event data. Secondly, not having

Architecture of a Digital Forensic Readiness Management System

the EAE store events in the database reduces the computational load on the EAE. Reducing the computational load is important because analysis is computationally intensive. The use of a database to log events allows for arbitrary queries to be performed against event history – something that may be necessary or useful in DF investigations.

For the sake of abstracting communication, alerts are also not sent directly from the EAE but rather through a communications handler. The communications handler allows for alerts to be sent through different forms of communication, for example, email or SMS. Whenever an alert is sent to the communications handler, it is also stored in an encrypted form in a database. This is done to have a record of all alerts that were detected by the EAE. In the case of the communications handler failing, it will still be possible to determine what alerts were triggered at what time by querying the database.

The EAM works in the same way as a SEM. Indeed, a SEM may perform the function of the EAM in the architecture, provided the SEM meets access control requirements which are discussed later in Section 10.4.3. In summary, the EAM satisfies requirements 1 to 5 in Table 9.

10.4.2 Digital Forensic Readiness Information Management Module

The primary purpose of the DFR information management module (DFRIMM) is to make the information required for DFR purposes available to the appropriate staff. Staff that need to work with the information stored in the DFRIMM are required to become users of the DFRMS. The DFRIMM allows for the management of such DFR-related information through the creation, editing and deletion of the items mentioned in Section 10.3.2 above, namely: policies, procedures, DF and incident teams, training requirements and organisational structure. These are requirements 6 to 16 in Table 9. The DFRIMM also has access to the device, system and business processes information used in the Event Analysis Module in order to manage training requirements. A diagram of the DFRIMM components is shown below in Figure 29.

Architecture of a Digital Forensic Readiness Management System

In the sub-sections below we detail how the DFRIMM handles the management of documentation for policies, procedures and organisational structure. With regard to DF teams, incident teams and training requirements, we show how the DFRIMM goes beyond document management and includes other functionality. In addition to the requirements drawn from the literature, we include functionality for leave management and an investigation archive. These are also discussed in the sub-sections below.

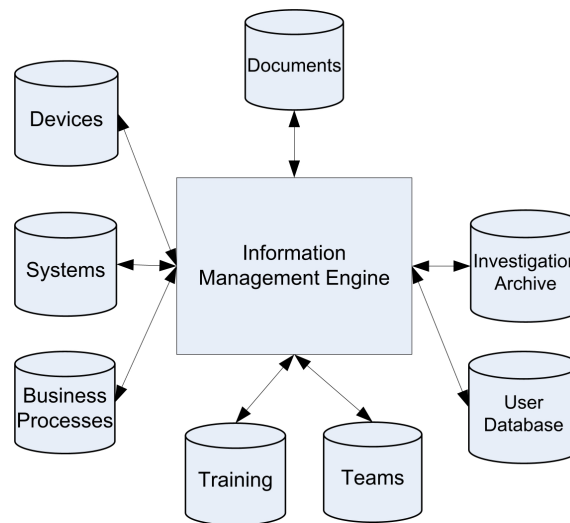


Figure 29 – Figure illustrating components of the DFRIMM

10.4.3 Management of Documentation

The DFRIMM stores policies, procedures and the organisational structure as electronic documents. In this regard, the DFRIMM serves essentially as a document management system for these documents. Document management can be defined as the automated control of electronic documents through their entire life cycle within an organisation (Cleveland 1995, p.3). Cleveland further notes that document management allows organisations “to exert greater control over the production, storage, and distribution of documents, yielding greater efficiencies in the ability to reuse information” and “to control a document through a workflow process” (Cleveland 1995, p.3). In large organisations that are likely to use a DFRMS, policies, procedures and organisational structure documents are likely to follow a formal workflow process in their creation and modification, making this functionality particularly useful.

Architecture of a Digital Forensic Readiness Management System

The need for document management stems from the requirements in the literature – to be specific, requirements 10-15 in Table 9. Incident response and escalation procedures, however, require decisions to be taken by staff. We believe that, in addition to the requirements in the literature, it should be optional for the DFRIMM to record such decisions. Recording these decisions makes it possible to determine if procedure was followed correctly. It also allows for review during post-incident analysis or evaluation as required by Carrier and Spafford’s framework (Carrier & Spafford 2003, p.12) mentioned in the Section 3.1.2.3. Kurowski and Frings (2011) have noted that the documentation of incidents can also prove a valuable asset to DF investigators. We do not make this functionality mandatory since the recording of decisions may create an administrative overhead to incident and escalation procedures that hampers their effectiveness. Depending on how the decision recording functionality is implemented, it may also force an organisation to adopt a workflow that is not optimal for the organisation. We therefore leave it to organisations to weigh the pros and cons of this functionality in their own environment.

Next, we discuss training management.

10.4.4 Training Management

The training management functionality in the DFRIMM serves to ensure that management is aware of the various training and skills available to them through trained staff members. Training management functionality records not only training completed by staff members but also the training currently underway, as well as the cost associated with training.

When devices, systems and business processes are added to the DFRMS they must have training requirements, including a possible null requirement, associated with them. This enables management to ensure that the requisite skills are available for all devices, systems and business processes by matching the skills required with the skills available. Where skills are not available for devices, systems or business processes, management can then attend to this.

Architecture of a Digital Forensic Readiness Management System

While the requirement from the literature is to record current and past training (see requirement 8 in Table 9), we believe the DFRMS should, where possible, also store available training courses and allow managers the ability to select appropriate training for their staff as training requirements change.

10.4.5 Digital Forensics and Incident Response Team Management

The DFRIMM allows for the creation of digital forensics teams, that is, the digital forensic investigators that are required to work together in teams for a specific purpose. For example, a group of DF investigators with the skills necessary to investigate incidents on the organisation's enterprise resource planning (ERP) software may be grouped together to form a team. In order to compose or create a team in the DFRIMM, all members of the team must be represented as staff members in the DFRIMM. Management can then select them from within the DFRIMM. In this way management is able to check their skills and training when creating teams and ensure that the teams are composed appropriately.

The same rationale and process applies to incident response teams. The only difference with incident response teams is that responders are likely to not all be DF staff. For example, a database administrator (DBA) may be part of an incident response team if, say, the database was to be shut down as part of the response to an incident. The DBA's manager may thus also need access to the training management functionality of the DFRIMM to update the DBA's DFR-training. As Lamis (2010) points out, incident response must proceed in a forensically safe manner. This implies that incident responders outside of DF staff may need some level of training to appreciate basic DF concepts, such as the chain of evidence.

Leave management, as mentioned, is a feature not found in the literature on DFR, but which we include in the DFRMS and discuss next.

Architecture of a Digital Forensic Readiness Management System

10.4.6 Leave Management

The leave management function in the DFRIMM allows management to administer the leave of staff involved in DFR. The reason for managing leave is that DFR can be negatively impacted if staff that possess certain skills are not present when their skills are needed. For example, consider the case where there is a single DF staff member that is trained to extract data in a forensically sound manner from the type of database used by the payroll system. If that staff member is on leave, the ability to be forensically ready for incidents involving the payroll system is severely hampered. The leave management functionality therefore brings this increased risk to the attention of management.

When considering leave for the staff member, management can see the skills and training that the staff member possesses and the devices, systems, business processes and teams the staff member's absence impacts. This is because, as previously mentioned, devices, systems, business processes are associated with skills and training requirements. The leave management functionality of the DFRIMM can then determine what is affected by linking the staff member's training and skills with the skills and training required for different devices, systems, business processes. In the example given, a manager may approve the staff member's leave request so that it does not fall within a payroll run.

10.4.7 Investigation Archive

The investigation archive in the DFRIMM serves as a secure storage location for potential evidence that DF investigators and/or incident responders may come across in their initial response to an incident. If an incident warrants a full investigation it is likely that DF analysis tools will be used to for proper analysis. The investigation archive is a convenience to DF investigators and incident responders and not a replacement for DF analysis tools. The convenience of the investigation archive lies in the fact that it allows appropriately authorised investigators, responders and management access to the same evidence or information when making decisions in response to incidents.

The investigation archive is encrypted and/or digitally signed to ensure that evidence is not tampered with. Access to the investigation archive is moderated through the access control module of the DFMS, which is discussed next.

Architecture of a Digital Forensic Readiness Management System

10.4.8 Access Control Module

The access control module (ACM) governs access control for all other modules in the architecture. The ACM is based on an underlying access control model which it uses to determine if users are allowed to access data or execute commands within the DFRMS. Records of user names, and the rights users possess, are stored in a database since in a large organisation there are likely to be many users. We do not mandate a particular access control model, such as mandatory or role-based access control for the DFRMS. The modular design of the architecture necessitates that the ACM should be interchangeable with an ACM based on a different access control model without significant changes to the other modules in the system.

The model chosen for the ACM should also be able to cater for the access control requirements that are peculiar to the DFRMS. One of the assumptions in the design of the DFRMS architecture is that users of the DFRMS may not all be trusted. To illustrate this concept, consider the following scenario. User X is a user of the DFRMS who has rights to subscribe to alerts. He is suspected of being complicit in fraud involving a financial application. As such, an alert has been defined for each time he logs into the financial application server. Since User X can see alerts and subscribe to them, it would not make sense for User X to see the alert defined for him. The ACM therefore has to provide the ability to hide alerts from users who would otherwise be able to see them. This also implies that the alert definition syntax must include the ability to specify which users should be blinded to the alert. In this scenario User X may be an IT Security staff member that makes use of the DFRMS, or indeed, even a DF staff member. The access control requirement is peculiar in this case since in most other monitoring software, such as SEMs, the ability to blind high-level users is not common.

The ACM must not only blind users from seeing specific alerts within a list of alerts, but must stop some users from discovering certain features and functionality of the DFRMS. For example, low level users that do not make use of the EAM should not be able to access the EAM and view its capabilities. This may provide less trusted staff valuable information on possible ways to circumvent monitoring and is in keeping with the principle of least privilege. The principle of least privilege states that a user should be

Architecture of a Digital Forensic Readiness Management System

given no more privilege than is necessary to perform a job (Ferraiolo & Kuhn 1992, p.562). Not allowing lower level users to make use of the EAM also implies that the ACM may be more tightly coupled with the user interface module than other modules.

Thus far we have discussed the ACM's role in the EAM. The ACM also plays a role in the DFRIMM and costing module. In the DFRIMM the ACM controls access to policy, procedures and the organisational structure documentation. The ACM ensures that only users with appropriate privileges are able to create, edit or delete documents. It does the same with team management by making sure that unauthorised users cannot create, edit or delete teams. Access to training and leave management and the investigation archive is also controlled by the ACM.

In the costing module the ACM makes sure that cost information is only available to the appropriate individuals. The costing module may contain sensitive financial information, such as salaries etc., therefore it is important that users are restricted to viewing only information that they would see in the ordinary course of their jobs.

The user interface module is described next.

10.4.9 User Interface Module

The user interface module (UIM), as its name suggests, provides users with a graphical user interface to the other modules. It is the only way that ordinary, non-administrative users interact with the DFRMS. The UIM is not tightly coupled with the EAM, DFRIMM, and costing module and therefore abstracts the user interface, or front-end, from the data processing modules, or back-end of the DFRMS.

An important function of the UIM is to record the actions of users in the DFRIMM. This provides an audit trail which can be used as evidence in the event of misuse in the DFRMS itself. User actions are stored directly in a database which stores the data in encrypted form. Administrative users have the ability to directly access the databases used by modules in the event of serious errors; however, user logging on the databases themselves should be enabled to record such actions.

Architecture of a Digital Forensic Readiness Management System

10.4.10 Costing Module

As mentioned earlier in Section 10.3.3, the costing module (CM) should provide a means, perhaps through TDABC, by which the cost of DFR measures can be determined. The cost of such measures may include, *inter alia*, the cost of staff, equipment or infrastructure and training. In order to determine such costs, cost information needs to be recorded where necessary. Cost information may be contained in the databases that are used for the DFRIMM. The CM therefore needs access to the following: training data, business process data, teams defined in the DFRIMM, as well as device and system data.

In the next section we conclude the chapter.

10.5 Conclusion

In this chapter we presented the concept of a digital forensic management system (DFRMS) that assists in the management of DFR in large organisations. We provided an architecture that can be used to build a DFRMS and based the architecture on requirements drawn from the available literature on DFR. To this end, a thorough search of the literature was conducted, the results of which were also presented and discussed. The architecture is modular in nature and contained five modules which functioned relatively independently from one another. The modules are: the event analysis module (EAM), DFR information management module (DFRIMM), costing module (CM), access control module (ACM) and user interface module (UIM). Each module was discussed, including how the module addressed the requirements from the literature that were presented earlier in the chapter. In certain instances the architecture went beyond the requirements in the literature, by including, for example, leave management as an element of digital forensic readiness.

In the short chapter that follows, we provide a more general discussion of the architecture presented in this chapter and also illustrate scenarios in which the architecture can be useful.