COMPUTERS & SECURITY XXX (2009) 1–10

available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Information security: The moving target

M.T. Dlamini[a,*], J.H.P. Eloff[a], M.M. Eloff[b]

[a]Information and Computer Security Architectures Research Group, Department of Computer Science, University of Pretoria, South Africa
[b]School of Computing, UNISA, Pretoria, South Africa

ARTICLE INFO

Article history:
Received 21 November 2007
Received in revised form
1 October 2008
Accepted 26 November 2008

Keywords:
Information security
Information security topics
Information security trends
Security breaches
Security journals

ABSTRACT

Information security has evolved from addressing minor and harmless security breaches to managing those with a huge impact on organisations' economic growth. This paper investigates the evolution of information security; where it came from, where it is today and the direction in which it is moving. It is argued that information security is not about looking at the past in anger of an attack once faced; neither is it about looking at the present in fear of being attacked; nor about looking at the future with uncertainty about what might befall us. The message is that organisations and individuals must be alert at all times. Research conducted for this paper explored literature on past security issues to set the scene. This is followed by the assessment and analysis of information security publications in conjunction with surveys conducted in industry. Results obtained are compared and analysed, enabling the development of a comprehensive view regarding the current status of the information security landscape. Furthermore, this paper also highlights critical information security issues that are being overlooked or not being addressed by research efforts currently undertaken. New research efforts are required that minimise the gap between regulatory issues and technical implementations.

1. Introduction

In the early days of computing, security breaches mainly included viruses and worms that would flash a message or advertisement on the screen without causing any serious damage to the information or systems being used. However, rare cases of attacks with the potential to harm information did occur, such as the Friday 13th virus which was set to erase all the information on infected disk drives on a certain Friday 13th late in the 1980s (Denning, 1991). As times changed, attacks also changed. Since the turn of the century, information security breaches have gained an unprecedented potential to impact negatively on businesses' reputation, profitability, customer confidence and overall economic growth (Romer and White, 2006). Cybertrust (2005) argues that this problem is two-fold: firstly it is due to the increase in economic and political uncertainty and secondly to the pressure from consumers and regulatory bodies.

As an example, a security breach such as the leakage of credit card information can imply an enormous damage to card payment companies due to the cancellation and re-issuing of compromised cards. This could also cost millions of dollars in penalties to regulatory compliance bodies. The case of a gang of Europeans who cloned 32 000 credit cards worth £17 million was reported in the Computer Fraud & Security News (2007) as the biggest (yet) uncovered credit card fraud. This is just a glimpse of losses related to today's threats.

It is therefore very important for companies to notice that their strength in attaining and sustaining competitiveness in the highly volatile, demanding and uncertain markets lies in

* *Corresponding author*. Information and Computer Security Architectures Research Group, Department of Computer Science, University of Pretoria, Lynnwood Road, Hatfield, Pretoria, Gauteng 0002, South Africa. Tel.: +27 124 203 035.
E-mail addresses: mdlamini@cs.up.ac.za (M.T. Dlamini), eloff@cs.up.ac.za (J.H.P. Eloff), eloffmm@unisa.ac.za (M.M. Eloff).
0167-4048/$ – see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2008.11.007

their ability to securely protect their information assets and IT infrastructure. It is not by mistake that information security has become a lingua franca not only to the world of computing, but also to various other industries. Multiple workshops and conferences such as IFIP/SEC (2007), NSPW (2007), USEC (2007), and WEIS (2007) have surfaced recently with the sole aim of discussing information security issues.

Does this mean information security is a new field or just another ''fad''? No, information security is neither new nor a ''fad''. What is new is its broader focus and wider appeal. For a long time most organisations would not recognise the importance of securing the infrastructure that holds and transmits their strategic information. Information security has been treated as a by-product, if not as a ''necessary evil that hinders productivity'' (Conray-Murray, 2003). Organisations would do it merely because everybody else is doing it. However, slowly but surely information security is getting into the forefront of things, and has been promoted from a by-product to an integral part of business operations (Conner and Coviello, 2004).

This paper gives an overview of the following:

- Where did information security come from? (the past)
- How did it get to where it is today? (the present)
- In what direction it is heading? (the future)

Information security is not about looking at the past in anger of an attack once faced; neither is it about looking at the present in fear of being attacked; nor about looking at the future with uncertainty about what might befall us. Security experts must be alert at all times. The aim is not to scare people but to make them aware of how information security has evolved over the past five decades. As remarked by Ormerod (2003), it is hard for anyone to navigate with a map if his or her current position is unclear. The future of information security can be realised only if its past and current positions are well understood (Botha and Gaadingwe, 2006).

Hence, Section 2 discusses the past events and Section 3 focuses on the current status of information security. This is followed by Section 4 which concludes this paper and provides ideas for future work.

2. Information security: then

Information security came into existence even before the invention of a computer. Rusell and Gangemi (1991) argue that information security is as old as information itself. From the time when information began to be transmitted, stored and processed, it required protection. This dates back to the time when human beings first learned how to write. Denning (1999) takes us back to the first century when Julius Caesar devised a secret code to protect (confidential) messages sent to his friends from being intercepted.

In the 1840s when the telegraph was invented (Rusell and Gangeni, 1991), an encryption code was developed to safeguard the secrecy of the transmitted telegrams. This was followed by the invention of the telephone and a year later legislation prohibiting wiretapping was put in place. Information security has moved from protecting the secrecy of hand written messages to telegrams, to telephone conversations and later to the world of computing. Information security originated with a main concern of protecting the secrecy or confidentiality of transmitted data and information.

The 1940s up to the 1950s marked the dawn of computing, when the first-generation computers came into existence. This was followed by the era of mainframe computers when only a few operators were permitted to use these computers. Other users would submit their jobs to the operator through protected slots (batch processing). The key security issue during this era was ensuring that only the privileged computer operator (one user one computer) would have access and that the physical computer was not stolen or damaged by outsiders. The scope of security gradually increased from the protection of secrecy or confidentiality of information, businesses' reputationructure (mainframe computers) that processed the information and storage media. Physical security was the basic principle underlying all security of computer systems.

Mainframe computers were isolated stand-alone units and networks were non-existent back then. Human messengers or physical mail was used to transfer programs and their data between computers. The only threat related to the transmission of information was that storage media could be lost or stolen. Even though it would take days to get information or data to its destination, data was safe.

The late 1960s until the early 1970s mark the beginning of dumb terminals. These enabled users (multiple users – one computer) to access and use remote data. This innovation introduced a new risk to remotely held data. Data could be accessed by unauthorized people or outsiders. Elementary physical security could not deal with this new risk. Therefore user identification and authentication came into play in the early 1970s. Physical access to terminals was screened by a security officer before the user could start the identification and authentication process. Since there were few terminals it was easy to keep track of all logged-in users and their activities.

However, since there were no security policies in place to enforce the use of strong passwords, password cracking was a big threat at this time. Password sharing posed another major problem. Guest and anonymous logins were still acceptable, as outsiders without much identification and authentication could access only limited resources inside the network.

The era of dumb terminals was succeeded by that of mini computers. The introduction of mini computers marked the beginning of networks, time-sharing and multi-user systems which changed the rules of the game. The number of people with computer know-how increased with the drop in prices of modems and terminals. Access controls were introduced to prevent users from interfering with one another's workspace. The work of Harrison, Ruzzo and Ullman (the HRU model) was the pioneer of access controls. This was followed by the Bell-LaPadula confidentiality model for Multics (Pfleeger and Pfleeger, 2007) and digital signatures from around the late 1970s to early 1980s. The Biba Integrity model was introduced and built on the Bell-LaPadula model (Sural, 2006). Over and above confidentiality, the concern for integrity came on-board.

Please cite this article in press as: Dlamini MT et al., Information security: The moving target, Comput. Secur. (2009), doi:10.1016/j.cose.2008.11.007

Also in the early 1970s public key cryptography came into existence. The Data Encryption Standard (DES) was adopted by the then National Bureau of Standards (NBS) of USA, which is now called the National Institute of Standards and Technology (NIST). This is around the same time that the ARPANET began, which aimed at providing a reliable and robust network to ensure the availability of computer systems (Denning, 1999). This innovation introduced a new dimension for the protection of information, and the goal posts were again moved on. In response the US government passed the Privacy Act of 1974 to safeguard personal information recorded in government systems (Rusell and Gangemi, 1991).

The 1980s marked the introduction of personal computers and suddenly every user had his/her own computer (Rusell and Gangemi, 1991). Again the number of people with computer know-how increased. Companies began to automate their operations and new security threats emerged as critical corporate data was now stored on easily accessible secondary storage. The scope of information security further widened. Hence, the 414 gang, the intruder (Markus Hess) who broke into computers at Stanford campus in the USA and the West German programmer who broke into the US military computers to steal documents were reported to be among the first intruder break-ins (Denning, 1991; Stoll, 2000).

This decade marked the rise of computer viruses, which spread through the use of diskettes. Denning (1991) reported viruses called ''Elk Cloner'' and ''The Brain'' to be among the first viruses ever created. The former was created by Rick Skrenta, targeting Apple II disks, and would display a poem on the screen. The latter of the two viruses flashed an advertisement for a Pakistani company and is believed to have been the work of two Pakistani brothers. Denning (1991) also cited Robert Morris to have created the first worm in 1988, arguing that even though it was harmless, it produced a massive scare. These were just a minor annoyance to the user but did not really do any harm to the information stored or processed, or to the infrastructure. Microsoft Windows and Local Area Networks (LANs) emerged in this decade.

The USA government issued the Computer Fraud and Abuse Act of 1984 to prosecute and establish harsh penalties for offenders (creators and authors of computer viruses). This Act came into practice following the conviction of Robert Morris, author of the first Internet worm (Russell and Gangemi, 1991; Denning, 1991, 1999). It was followed by the Computer Security Act of 1987, also from the USA, which dealt with the training of security personnel involved in the processing of sensitive information.

The late 1980s also saw the introduction of anti-virus software. Carey (2008) argues that the European Bernt Fix in 1987 made the first ever anti virus. In 1988, Alan Solomon, of Great Britain released an anti -virus software called Dr. Solomon's Anti-Virus Toolkit.

What was conceived in the late 1960s and born in the early 1970s as the ARPANET grew in the 1990s as LANs and WANs merged in distributed systems. The 1990s was dominated by open systems and mobile computing. More and more personal computers connected to the Internet. This innovation brought new risks, as would be expected since open systems would also be open to abuse (Denning, 1991). The hacking community created freely available hacking tools, and hence virus and worm attacks intensified and script kiddies started showing their faces. Anti-virus products were a prime solution.

Carey (2008) claims that by the end of 1990, there were approximately nineteen anti virus software environments including Symantec's Norton Anti Virus, ViruScan by McAfee; and IBM's Anti Virus. However, there are conflicting views as Pearson (2007) claims that Norton and ViruScan were among the first anti-virus environments created to combat viruses and worms.

Towards the end of the 1990s attackers changed from using worms and viruses to more sophisticated attacks. The introduction of distributed denial of service and malicious code attached to business emails and web pages shifted the focus to gateways. This saw the introduction of filtering firewalls. Perimeter security came into existence to provide a wall around networks and keep outsiders out. But as the use of the Internet intensified, network boundaries disappeared and perimeter security vanished.

As we entered the 21st century, things changed. Attackers started hacking for financial gains and not just to show-cast their skills. IT infrastructure became pervasive in almost all industries (known as the era of pervasive computing). Every second word now began with an E, for example E-commerce, E-voting, E-business, E-government, etc., because everything had gone electronic. As all sorts of devices came on-board (Personal Digital Assistants, Smart phones, Laptops, Tablet PCs, etc.), it became difficult to clearly define a computer. Mobile computing (Bluetooth and Wi-Fi) also emerged to complicate things even further. Online payment systems and the usage of credit cards became highly popular and web-based applications intensified. However, the fact remains that all these new developments in technology were vulnerable and like all other good things came with side effects (risks).

3. ….and Now

The 21st century innovations and developments came along with a strong dependency on IT infrastructure. This opened new and attractive doors for the hacking community. Attackers have evolved from computer enthusiasts to professional hackers (Gelbstein, 2006). Bruce Schneier quoted in Anderson (2008) argues that ''it is only amateurs who still target machines; career criminals now target people who operate them not just for fun but for financial gains''. Attackers have matured from using hacking skills to show that they can circumvent the authentication process to access each other's files to use them in the theft of confidential information. This has resulted in information security threats like identity theft, social engineering, phishing, etc which can easily compromise authentication and authorization credentials. Nowadays the motive of an attacker is financial gains and in order to evade the ''long arm of law'', he/she will do everything to cover his/her tracks. As a solution and in addition to the authorization and authentication credentials, verification of users became necessary for access. Banks introduced chip-and-pin. Non-repudiation has since become a critical issue of the 21st century.

Please cite this article in press as: Dlamini MT et al., Information security: The moving target, Comput. Secur. (2009), doi:10.1016/j.cose.2008.11.007

Viruses and worms have evolved from minor annoyances to having catastrophic impacts and can infect thousands of machines in seconds (Zetter, 2003; Petreley, 2004). Creators of these threats have opted for a new twist on an old trick (MacMillan, 2008). Simple attacks have matured to become sophisticated, automatic, subtle and very hard to detect (Schneier, 2003; Carey, 2008). There is also the evolution of spam and phishing from email to SMS (short message service) and MMS (multimedia message service) technology in mobile phones (Symantec Internet Security Threat Report, 2007). Attackers are on the verge of re-inventing the wheel. They use old tricks in new twisted ways (MacMillan, 2008) and therefore the history of information security is as critical as the uncertain road ahead.

The future of information security remains clouded with numerous uncertainties. However, two things remain certain – IT infrastructures are vulnerable and motivated attackers are always ready to exploit these vulnerabilities. It is therefore critical that securing information and infrastructures should not be considered in fear of inevitable attacks, but in preparation for the uncertain future. This requires innovative ideas and insightful analysis of security issues to appropriately respond to the challenges posed by new developments. Another challenge is that as information security moves to respond to new threats in current and future environments, it must also protect against well-known threats. The goal posts are not only moving, but they also widen each time, making it very difficult to protect information and its infrastructure.

3.1. *The current information security trends*

Despite several studies aimed at providing much needed statistical information on security trends and issues, there is still an urgent need to find one that is complete and reliable. CSIA (Cyber Security Industry Alliance) (CSIA, 2007) compiled a list of disparate sources of information and statistics related to information security issues and their trends. This includes an overview of the work of Symantec, Sophos, Deloitte global security survey, Ernst & Young global information security survey, CSI/FBI computer crime and security survey, SANS institute, etc. However, most of these target the US and UK communities and very few have the world community as their target. Security experts can gain a good understanding of the current information security trends and issues by using the results of the above surveys. It is unfortunate that there is still (to the authors' knowledge) no work that pays attention to the aggregation of the above surveys to get a holistic picture of the global information security landscape.

To further develop a good understanding of the current information security landscape, this paper outlines the following two phases of research as conducted for this project:

- Phase 1 monitored, assessed and analysed articles covered in the following four journals: Computer & Security, Computer Fraud & Security, IEEE Security & Privacy and Information Management & Computer Security. The main aim is to identify the critical issues currently being addressed by security professionals to gain a complete picture of today's information security posture. The survey is based on publications for the years 2005 until December 2006. The question can be asked why these four journals? There are many journals and publications available today which focus on information security related issues. However, the authors of this paper wanted to include journals that represent both an academic (Computers & Security, IEEE Security & Privacy, Information Management & Computer Security) as well as a business (Computer Fraud & Security) view on the matter. Furthermore, because the authors wanted to focus on identifying trends it was important to include journals that are well established and have been available for a long enough time e.g. Computers & Security. It was also decided to only include journals that have information security as its primary focus.
- Phase 2 made an analysis of the 2006 report issued by the Computer Security Institute/Federal Bureau Investigations (CSI/FBI) on computer crime and security (Gordon et al., 2006) as well as the SANS Institute (2006) report. The reasons for including surveys conducted by these two institutes are as follows: both institutes have delivered for many years a service to the information security community in the large; they both provide a wealth of security related content free to the public; both institutes have extensive research archives.

3.1.1. *Limitations of the study*

3.1.1.1. Phase 1. All the publications seem to be more common in university libraries than in chief security officers' offices. Hence, it is unlikely that this approach will capture the true picture of the current information security landscape. Whilst the publications to a lesser extent reflect current research, they do not really reflect on the breaking security issues faced by information security practitioners. This is because the publications go through a long peer review process which adds a long time lag to the publication route and hence, they tend to rather deal with long term issues than short-term issues. The publications seem to focus more on full papers than the small section on breaking security issues. As a result they are not so responsive to the current security trends and issues. Hence, they tend to be a following rather than a leading indicator of information security trends. However, the publications are published almost monthly and contain articles written and reviewed by experts in the information security field which makes them relevant. They also to a certain extent reflect the latest developments in the information security field. Although these four publications do not at all represent the whole spectrum of information security publications, the authors believe that assessing them can provide valuable insights into the current state and trends of information security.

3.1.1.2. Phase 2. The SANS Institute and CSI/FBI reports are both based on survey respondents. There are several drawbacks in such surveys which involve survey respondents, more especially security experts. Firstly, survey respondents tend to be biased when reporting security breaches in fear of the consequences of legal liability, and of damaging customer confidence and company reputation. Organisations usually do not report or reveal exact security breaches as they occurred

Please cite this article in press as: Dlamini MT et al., Information security: The moving target, Comput. Secur. (2009), doi:10.1016/j.cose.2008.11.007

(Eppel, 2005). Secondly, criminals hide their successful attacks which makes some security breaches go undetected and never accounted for in such survey results. Thirdly and final, vendors exaggerate the risk to market their products (Eppel, 2005). Hence, CSIA (2007) argues that surveys may provide valuable insights but there are doubts about their authenticity, correctness and completeness.

It is therefore very difficult to get a true and comprehensive view of the current state of information security based on the results of such surveys. However, to remove such doubts the results from the survey respondents will be aggregated with those of Phase 1 to help in developing a holistic picture of the current security trends and issues.

3.1.2. *Data collection*

This section investigates the computer and information security issues found in the Computers & Security, Computer Fraud & Security, IEEE Security & Privacy and Information Management & Computer Security publications for the year 2005 and 2006.

3.1.2.1. *Topics covered in the journals (phase 1)*. The data collection process started with a brainstorming session where all sorts of information security related topics were identified. These were then grouped into broad category topics to accommodate most of the topics identified in the brainstorming sessions. For example, every topic that dealt with surveillance cameras, fences, security guards and the likes were grouped as ***physical security***. Information security budgets, spending, culture, behaviour and anything that pertains to the management of information security were categorized as ***information security management***. The same strategy applies to all the other broad topics. All the topics that appear not to be part of any of the broad topics were categorized as ***other***. This category included topics like: security outsourcing; critical infrastructures; anonymous protocols and end user security to name just a few.

Even with this general option ***other***, there are certain limitations of the study as some topics could sometimes fit into more than one broad category. For example, the case of digital forensics and legal issues often overlap. To correctly categorise such issues, the abstract and keywords of an article would be read to determine its key theme. If still unclear, the conclusion would be consulted. The same technique applies for topics that are unclear or ambiguous. What must be noted though is that the categorisation used in this study does not represent a standard scientific categorisation, but solely the views and opinions of the authors.

3.1.2.2. *Results obtained from the journals*. This sub-subsection outlines the profile of articles published in all four publications over the period investigated. Some of the publications (i.e. Computers & Security and Computer Fraud & Security) contain a section on brief news or short discussions that would otherwise not qualify to be called full articles. These are also included in the survey results because they provide qualitative information about current security issues. Fig. 1 summarises the amount of coverage given to each topic by all the journals included for this survey.

When investigating each of the journals separately, it is interesting to note that different topics were emphasized by each journal.

Table 1 lists the top five topics in each of the journals in priority order with 1 being the most published topic for that specific journal.

Outstanding in the results of the Computers Fraud & Security publication is that risk management took the lead with 67 articles, followed by legal and compliance regulatory issues at 40, digital forensics at 23, network security at 21 and physical security at 20 to constitute the top five.

In the Computers & Security publication, articles on legal and regulatory compliance issues were more than all the other categories at 56, followed by digital forensics at 30, other at 27, risk management at 22 and information security management at 14 closing the top five most discussed topics.

The IEEE Security & Privacy publication focussed on amongst others on software security with 35, privacy at 28,

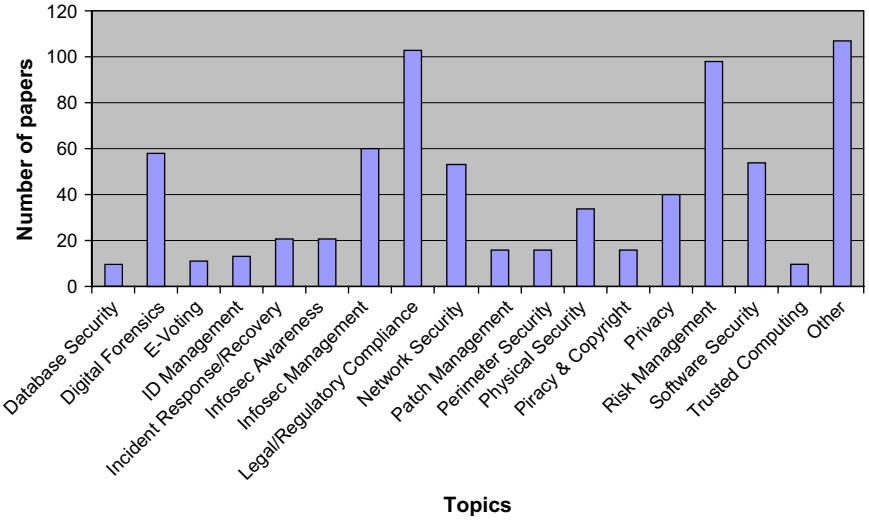

Fig. 1 – Importance of topics across all journals.

Please cite this article in press as: Dlamini MT et al., Information security: The moving target, Comput. Secur. (2009), doi:10.1016/j.cose.2008.11.007

Table 1 – The top five topics in all the four publications.

	Computer Fraud & Security	Computers & Security	IEEE Security & Privacy	Information Management & Computer Security
Digital Forensics	3	2		
ID Management				5
Information Security Awareness			5	
Information Security Management		5	4	1
Legal & Regulatory Compliance	2	1		5
Network Security	4		4	4
Other		3	1	2
Perimeter Security				3
Physical Security	5			
Privacy			3	4
Risk Management	1	4		3
Software Security			2	3

then network security and information security management are tied at 23 and information security awareness at nine.

Lastly in the Information Management & Computer Security publication information security management took the lead at 12, with *other* at 11, followed by risk management, perimeter security and software security tied at five, then network security and privacy tied at four and in the 5th place legal and regulatory compliance and identity management at three.

3.1.3. *Surveys of existing CSI/FBI and SANS reports (phase 2)*

In this subsection the study considers two well established surveys that had been gathering statistics and trends on information security for many years. These are the CSI/FBI computer crime and security survey and the SAN institute survey. However, the study at hand only focuses on the 2006 results.

The CSI/FBI survey has been gathering information security statistics for the past 12 years and they have developed significant experience in the field. Their results are based on the answers of survey respondents, which mainly consist of security practitioners from almost all industrial sectors in the United States. The US respondents' answers may not represent the true picture of information security worldwide, but they do provide valuable insights. The 2006 CSI/FBI data on the most critical security issues for 2007 and 2008 is used by the authors to compile a graph as shown in Fig. 2.

The SANS Institute (2006) report is based on twenty most respected leaders in cyber-security who developed a list of ten most important trends in predicting the future of information security. Unlike the CSI/FBI, the SAN Institute report is a good representation of the worldwide situation of information security because it involves not only the US security practitioners but cyber-security leaders from all over the world. The top five issues in both reports are summarised in the following table in ascending order.

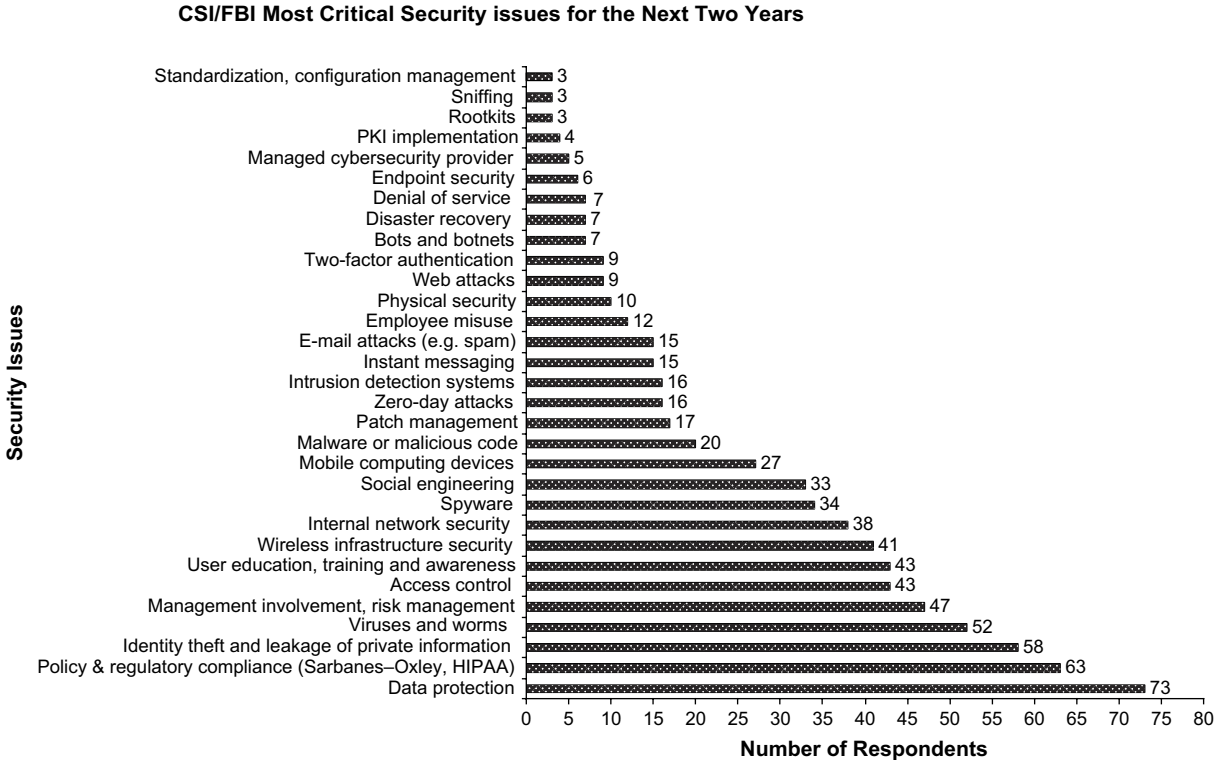

Fig. 2 – Graph drawn from statistics/data provided by CSI/FBI (Gordon et al., 2006).

Please cite this article in press as: Dlamini MT et al., Information security: The moving target, Comput. Secur. (2009), doi:10.1016/j.cose.2008.11.007

Table 2 – The top five issues of both security surveys.

CSI/FBI computer crime survey	SANS Institute Survey
1. Data Protection	1. Laptop or mobile hardware devices encryption
2. Policy and regulatory Compliance	2. Significant growth in theft of PDA smart phones
3. Identity theft and Leakage of private information	3. More legislation governing the protection of customer information
4. Worms and viruses	4. Increase in targeted attacks
5. Management involvement and risk management	5. Increase in cell phone worms

Table 2 shows data protection at the top of the CSI/FBI survey, followed closely by policy and regulatory compliance and placed third is identity theft and leakage of private information. These are the three hot topics which are so critical to information security. The issue of worms and viruses is no longer like it was in the early 1990s. This is because cyber criminals are now stealing credit and debit card numbers, trade secrets and personal identifiable information for financial gains. The issue of management is slowly moving up the list of security priorities.

On the other end of Table 2, the SANS Institute survey reports encryption of mobile devices as a primary concern, followed by the issue of growing theft of smart phones, and then the legislation for the protection of customer information to prevent identity theft and related threats. Perched third is the issue of the growing number of targeted attacks and the invasion of cell phones by viruses and worms rightly so because of the converging networks and the capacity of smart phones. More discussion on these and other results follows in next subsection.

3.2. *Discussion and analysis of results*

This section compares and discusses the results of the publications survey with the CSI/FBI and SAN Institute 2006 reports on the future information security predictions. Notable in the findings is that most of the publications are written by security experts for the computer and information security community. Hence, one would expect to find most of the articles on database security, physical security and many other issues directly related to security technologies. However, this is not the case. Does this mean information security has changed?

No, information security has not changed per se, but it has since gained a broader and wider focus. This has caused security experts to change their focus too. From the early days of computing, information security has been put in the hands of security experts, but of late things are changing – as are clear from the results.

The results show a strong emphasis on three aspects: legal and regulatory compliance, risk management and information security management. This indicates that the security responsibility is widening to also include risk managers, forensic specialists, compliance regulators and other stakeholders. This involves a major shift from pure reactive technical measures towards a more proactive strategic approach (Volker, 2007). Also in support of the study findings are the predictions of the 2006 CSI/FBI report which points towards a strategic approach. However, the SANS Institute (2006) report predicts an increase in encryption of mobile devices. The indication is that even with the move towards a strategic approach, technical measures are still as applicable as they were ten years ago.

The survey reveals that the Computers & Security publication put most emphasis on legal and regulatory compliance. In comparison to the others, legal and regulatory compliance is ranked second in the Computer Fraud & Security publication, third in the SANS Institute (2006) report, second in the CSI/FBI report and fifth in Information Management & Computer Security. Data protection, which is ranked first in the CSI/FBI report, also falls in this category. This shows that computer crime authorities around the world are working hard to find solutions for combating the rise in cyber-crime (Sophos, 2007).

Regulatory compliance goes hand in hand with legal issues as it ensures that standards are implemented and adhered to. Its main objective is to assess whether organisations have enough controls, are doing the right things, and are doing the right things the right way (Gelbstein, 2006). Regulatory compliance authorities enforce control by ensuring that organisations that do not comply with set standards face penalties and legal consequences and those that do, are awarded certificates in recognition. In as much as regulatory compliance enforces the use of appropriate security controls, its main target are the human factor of security.

The Computer Fraud & Security publication results show a main emphasis on risk management, which is ranked fourth in Computers & Security, fifth in the CSI/FBI report, third in Information Management & Computer Security and does not appear on the top five list of SANS Institute's (2006) report and the IEEE Security & Privacy publication. Information security experts are beginning to see the bigger picture. This is an indication that the debate is moving from an operational and tactical level towards a strategic level of risk management. However, this does not necessarily mean that the technical paradigm no longer has a role in information security.

Today's security threats are forcing organisations to become more adaptable and flexible with regards to the people, process and technology risks. It is through such risks that information security is a standard item on the agenda of senior management's meetings nowadays. This sets the scene and acts as the motivation for discussions on insurance in relation to secure information and its infrastructure.

The survey results further show that information security management is another focus area in the information security press. This topic is ranked first in Information Management & Computer Security, third in IEEE Security & Privacy, fifth in Computers & Security and CSI/FBI. However, it is not a high priority in the other publications. This could be due to several biases that could be as a result of the audience and the focus of the publications. Information security management is a critical factor to get information security issues discussed in board rooms. Furthermore, information security management is a means to a strategic information security approach.

Please cite this article in press as: Dlamini MT et al., Information security: The moving target, Comput. Secur. (2009), doi:10.1016/j.cose.2008.11.007

The survey results also show network security as another topic that has received attention in the information security press. It is ranked fourth in Computer Fraud & Security, IEEE Security & Privacy and Information Management & Computer Security publications. This issue is just as important nowadays as it has ever been as networks are converging with their inherent risks. It is therefore very critical for the information security experts to address network security issues. Again this is an indication that technical issues are still applicable in the current and future information security landscape.

The other issue of concern in the information security press is digital forensics; a critical issue ranked third in the Computer Fraud & Security, second in the Computers & Security. However, it does not appear in the other two publications, CSI/FBI and the SAN top five. Digital forensics connects the law and information security. It ensures that evidence collected on the crime scene gets to the courts in an unhampered or uncontaminated state to facilitate the apprehension of criminals. However, such initiatives are undermined by inappropriate penalties stipulated in current laws. Hence, many computer crime perpetrators have been given inordinately light sentences for serious crimes. For example, the UK's Information Commissioner (2006) reports that between 2002 and 2006, only two out of 22 cases resulted to penalties amounting to only about £5000. A call has since been made to raise cyber-crime penalties (Information Commissioner, 2006) and to increase the coordination between information security, digital forensics, government and law enforcements in order to best track and convict cyber criminals.

Ranked third in the CSI/FBI report is the issue of identity theft and the leakage of private information. Directly linked to identity theft and leakage of private information is privacy which is ranked third in IEEE Security & Privacy and Information Management & Computer Security. It is encouraging to see these issues being on the top five list of security issues being discussed. More so after Gunter Ollmann (cited in the editorial news section of Computer Fraud & Security, 2007), reported that on the black market identities are selling for much more than credit card numbers. This is another critical area that security practitioners need to look at in order to address current and future threats.

Software security is ranked second in IEEE Security & Privacy and third in Information Management & Computer Security but not covered in the other publications. Software security is a major issue that underlies insecure systems. The expectation would be to have more publications addressing software security.

The theft of laptops, smart phones, PDAs and other mobile devices is on the rise (SANS Institute, 2006). However, what attract most thieves are not just the devices per se but the data held in them. It is therefore no coincidence that the issue of laptop or mobile hardware encryption lay at the top of the five most important security trends of the report by the SANS Institute (2006). This is an effort to ensure that even if such devices get stolen, the critical and valuable data they hold will not be compromised. Moreover, the SANS institute reported legislation governing the protection of such data or information to ensure that organisations that lose or compromise such data would face legal consequences. Data protection, which is ranked first in the CSI/FBI report, also supports the SAN institute's findings. Preserving privacy, preventing identity theft and leakage of private information is critical nowadays.

Furthermore, the SANS report predicts an increase in targeted attacks and cell phone worms. The former is concerned with purposeful attacks mainly driven by financial motives. The latter shows that the target is moving towards new environments as it spreads to exploit cellular networks. The CSI/FBI report shows that worms and viruses will continue to be a big threat to information systems in the next few years. These threats are finding new exploits to infect and they are becoming increasingly sophisticated and thus hard to detect. Such threats cause the scope of information security to continue widening.

Physical security, information security awareness, identity management and perimeter security are also in the top five topics discussed even though not extensively. These are the issues that security experts are expected to be more concerned with. However, this is unfortunately not the case.

These research results show the current direction of information security. It is clear that information security research is moving towards a strategic approach. However, this is not a complete switch as technical measures remain applicable. The end result is that information security's focus is widening and deepening. However, several other issues remained overlooked or needs more emphasis by current research despite being critical for securing information. Such issues are discussed in the next section.

3.3. *Critical overlooked security issues*

The survey results show that only a few articles discuss information security awareness and training, incident response and disaster recovery and the human aspect of information security (social, cultural and ethical aspects of human resources and organisation policies). Organisations must understand that the best security technologies in the world cannot stop a social engineer impersonating legal users for access codes. Moreover, they cannot stop a stranger walking in an organisation empty-handed and emerging with a laptop full of sensitive data. It is for this reason that information security awareness campaigns have emerged as an important aspect of information security. A well-conducted awareness campaign can help teach and make users aware of emerging threats. This can also help to educate users on the right channels to follow in reporting security incidents. To remain effective, awareness campaigns must not be a once-off exercise, but they should be held periodically as new threats and countermeasures are introduced.

Incident response and recovery is in sixth place on the list of Computer Fraud & Security, whereas in the other publications it is nowhere near the top five. It also does not feature in the top five of either the CSI/FBI or the SANS report. After the 9/11 terrorist attacks one would have expected this topic to be among the top security issues being discussed. But this is not the case. This issue is very important in planning for the unthinkable disasters well in advance. For those vulnerabilities that can never be prevented (natural disasters), it is more beneficial to direct more resources to the recovery from loss, rather than to try and defend against them. Therefore incident

Please cite this article in press as: Dlamini MT et al., Information security: The moving target, Comput. Secur. (2009), doi:10.1016/j.cose.2008.11.007

response and recovery must be considered to secure information systems.

Another issue of prime concern is that of the human aspect of information security. Naturally human beings are fallible – between system designers and system users mistakes are inevitable. There is much that security design experts can learn from the designers of high reliability organisations (HROs) that embrace human fallibility (''to err is human''). Errors or failures are inevitable and are to be expected. Security design experts should learn more from errors and failures than from successes as the designers of HROs do. Reason (2000) argues that although the fallible human condition cannot be changed, the conditions under which human beings work can. Therefore, most studies must be devoted to research on how human beings interact with IT systems and how security problems arise from such interactions (cyber deviance). This can help build secure systems that will reduce errors and restrict their effects to a minimum or acceptable level.

To summarise all the findings, the current information security landscape is moving towards a more strategic approach. The strategic approach to information security management is nowadays commonly referred to as Information Security Governance. Theoharidou et al. (2005) contend that information security has emerged as a new paradigm that requires a multi-disciplinary approach.

4. Conclusion and future work

Information security has moved from the era of mainframe computers up to the current state of the complex Internet. With new developments and innovations, new risks came along. The survey results has shown that as we entered the twenty-first century, the scope of information security has widened and its focus is fast shifting towards a strategic governance one. Security issues now require a more coordinated and focused effort from the national and international society, governments and the private sector. It is no coincidence that the study shows a shift towards legal and regulatory compliance, risk management and digital forensic fields.

The survey's findings have also shown that most of today's security challenges are to a greater extent related to the human and organisational aspects (Anderson, 2007) of security. All indicators points to a multi-disciplinary approach in the future development of the information security discipline. However, as we move forward to address the new challenges it is also critical that we continue strengthening the technologies. New research efforts is required that minimise the gap between regulatory issues and technical implementations.

Acknowledgments

The support of SAP Research CEC Pretoria towards this research is hereby acknowledged. M.T.Dlamini is an intern at SAP Research and J.H.P. Eloff is a research collaborator with SAP Research. Opinions expressed and conclusions arrived at are those of the authors and not necessarily to be attribute to SAP Research.

REFERENCES

Anderson K. Convergence: a holistic approach to risk management. Network Security 2007;2007(5):4–7. Elsevier.
Anderson R. Security engineering: a guide to building dependable distributed systems. United States of America: Wiley Publishing, Inc; 2008.
Botha RA, Gaadingwe TG. Reflecting on 20 SEC conferences. Computers and Security 2006;25:247–56.
Carey L. The evolution of computer virus and anti virus protection. Available online at: http://www.identitytheftsecrets.com/the-evolution-of-computer-viruses-and-anti-virus-p.html; 2008 [accessed 14.07.08].
Computer Fraud & Security. IDs sell for much more than credit card numbers in the underground, editorial news. Computer Fraud and Security 2007;2007(12):2.
Computer Fraud & Security News. UK police bust fraud gang. Computer Fraud and Security 2007;2007(6):2. Elsevier Ltd.
Conner FW, Coviello AW. Information security governance: a call to action, corporate governance task force report of 2004, 2004.
Conray-Murray A. Strategies & issues: justifying security spending. Available online at: http://www.itarchitect.com/articles/NMG20020930S0002.html; 2003 [accessed 18.07.07].
CSIA. CSIA compilation of data sources for information on cyber security issues. Available online at: www.csialliance.org/resources; 2007 [accessed 13.08.07].
Cybertrust. Justifying security spending: how to make a business case for information security. Available online at: http://www.cybertrust.com/media/white_papers/cybertrust_wp_security_spending.pdf; 2005 [accessed 13.08.07].
Denning ED. Information warfare and security. United States of America: ACM Press; 1999.
Denning PJ. Computers under attack: intruders, worms, and viruses. United States of America: Addison-Wesley Publishing Company; 1991.
Eppel N. Security absurdity: the complete, unquestionable, and total failure of information security. Available online at: http://www.securityabsurdity.com/failure.php; 2005 [accessed 16.07.07].
Gelbstein E. Information security for policy makers: what it means- why it matters- what to do about it?. Available online at: http://www.unitarny.org/mm/File/Webinars/Unitar%20eg%20presentation%2030_08.pdf; 2006 [accessed 14.08.07].
Gordon LA, Loeb MP, Lucyshyn W, Richardson R. CSI/FBI computer crime and security survey 2006 report. Available online at: www.abovesecurity.com/doc/CommuniquesPDF/FBISurvey2006.pdf; 2006 [accessed 06.05.07].
Information Commissioner. What price privacy? the unlawful trade in confidential personal information, information commissioner's office. Available online at: http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf; 2006 [accessed 14.07.08].
MacMillan R. New rootkit uses old trick to hide, IDG news service. Available online at: http://www.pcworld.com/article/141300/new_rootkit_uses_old_trick_to_hide.html; 2008 [accessed 14.07.08].
Ormerod P. Sunday times article. Available online at: http://www.paulormerod.com/current.html; 2003 [accessed 05.05.07].
Pearson Education. Computers and the internet, fact monster. Available online at: http://www.factmonster.com/ipka/A0872842.html; 2007 [accessed 04.07.07].
Petreley N. Security report: windows vs. Linux, the register. Available online at: http://www.theregister.co.uk/security/security_report_windows_vs_linux/; 2004 [accessed 14.07.08].
Pfleeger CP, Pfleeger SL. Security in computing. 4th ed. United States of America: Prentice Hall; 2007.
Reason J. Human error: models and management. BMJ:768–70. Available online at: http://www.cs.up.ac.za/download.php/

AIP780/Papers/Reason_2000_Human_error_models_and_management_BMJ.pdf, 2000;320 [accessed 29.05.07].
Romer H, White W. Security inside out, oracle security solutions. Available online at: www.oracle.com; 2006 [accessed 19.07.07].
Rusell D, Gangemi GT. Computer security basics. United States of America: O'Reilly & Associates, Inc.; 1991.
SANS Institute. The ten most important security trends of the coming year. Available online at: http://www.sans.org/resources/10_security_trends.pdf; 2006 [accessed 04.07.07].
Schneier B. The speed of security. IEEE Security and Privacy 2003;1(4).
Sophos. Sophos security threat report July 2007. Available online at: http://www.tradepub.com/free/w_soph08; 2007 [accessed 13.08.07].
Stoll C. The cuckoo's egg: tracking a spy through the maze of computer espionage. 1st ed. United States of America: Pocket; 2000.
Sural S. Information security: brief history and current perspective. Available online at: http://egovstandards.gov.in/; 2006 [accessed 08.08.07].
Symantec Internet Security Threat Report. Trends for July–December 06. Vol. XI. Available online at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_emea_03_2007.en-us.pdf; 2007 [accessed 13.08.07].
Theoharidou M, Kokolakis S, Karyda M, Kiountouzis E. The insider threat to information systems and the effectiveness of ISO 17799. Computers and Security 2005;24:472–84.
Volker T. Security goes from tactical to strategic. Available online at: http://www.mydigitallife.co.za; 2007 [accessed 13.08.07].
Zetter K. Just say no to viruses and worms. Available online at: http://www.wired.com/techbiz/it/news/2003/09/60391?currentPage=all; 2003 [accessed 15.07.08].

Mr Moses Dlamini received his BSc Computer Science and Mathematics in 2002. In 2006, he received his Honours BSc Computer Science after working as a teaching assistant at the local university of Swaziland. He has also worked as an assistant lecturer at the University of Pretoria. He is now working towards finishing his MSc in Computer Science at the University of Pretoria.

Prof Mariki Eloff received a PhD Computer Science degree in 2002 and gained tertiary teaching experience by lecturing at various tertiary institutions in South Africa for more than 20 years. Since October 2002 she is appointed as an associate professor in the School of Computing at UNISA. She is a member of the College of Science, Engineering and Technology Executive and Research Committees at Unisa. She participated in many information security management research projects and contributed to the development of various information security-training modules for industry. She has presented research papers at international and national conferences mostly focusing on information security. She has assisted in the organisation and management of international conferences in information security. Mariki is the co-chair of the Information Security South Africa (ISSA) annual conference.

Prof Jan Eloff has been Head of the Department of Computer Science at the University of Pretoria, South Africa since October 2002. He is a full professor in Computer Science. He is a member of Technical Committee 11 (Information Security) of the International Federation for Information Processing (IFIP). From 2004 to 2007 he was the President of the South African Institute of Computer Scientists and Information Technologists (SAICSIT). Jan has published extensively in a wide spectrum of accredited international subject journals and he is a member of the Council for Natural Scientists of South Africa. He has received a B-rating from the NRF as a researcher who enjoys considerable international peer recognition for the high quality of his recent research outputs. Jan is the co-chair of the Information Security South Africa (ISSA) annual conference.

Please cite this article in press as: Dlamini MT et al., Information security: The moving target, Comput. Secur. (2009), doi:10.1016/j.cose.2008.11.007