CONTROLS FOR PROTECTING CRITICAL INFORMATION INFRASTRUCTURE FROM CYBERATTACKS

By

Tamir Tsegaye

201113929

Information Systems Honours Treatise (IFS503E)

Submitted in partial fulfilment of the requirements for the degree

Bachelors of Commerce Honours

in

Information Systems

for the

Department of Information Systems

at the

University of Fort Hare

Supervisor: **Prof. Stephen Flowerday**

September 2014

ABSTRACT

Critical information infrastructure has enabled organisations, including governments and businesses, to store large amounts of information on their systems and deliver this information via networks such as the internet. Users who are also connected to the internet are able to access various internet services such as e-commerce which are provided by critical information infrastructure. However, some organisations have not effectively secured their critical information infrastructure and hackers, disgruntled employees and other entities have taken advantage of this by using the internet as a medium to launch cyberattacks on their critical information infrastructure. They do this by using cyberthreats to exploit vulnerabilities in critical information infrastructure which organisations fail to secure. Once a vulnerability has been exploited, cyberthreats will consequently be able to steal or damage confidential information stored on systems, or take down organisationsô websites and prevent authorized users from accessing information. Thus, the confidentiality, integrity and availability of information will not be maintained. Despite this, risk strategies can be used to implement a number of security controls: preventive, detective and corrective controls, which together form a system of controls. This will ensure that the confidentiality, integrity and availability of information is preserved, thus reducing any risks to information. This system of controls is based on the General Systems Theory, which states that the elements of a system are interdependent and contribute to the operation of the whole system. Finally, a model is proposed to address insecure critical information infrastructure.

DECLARATION

I _____, hereby declare that:

- The work in this treatise is my own work, and this has been confirmed by uploading it to a plagiarism tool for evaluation.
- All sources used or referenced have been documented and recognised.
- This treatise has not been previously submitted in full or in partial fulfilment of the requirements for an equivalent or higher qualification.

Signature: _____

Date: _____

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Professor Stephen Flowerday for his expertise, guidance and helpful advice, which have contributed towards this research project, as well as my family for their support. The financial assistance of the National Research Foundation is hereby acknowledged. Opinions expressed and conclusions arrived at are those of the author and are not necessarily to be attributed to the National Research Foundation.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

CHAPTER 1: INTRODUCTION

1.1 Background

Cyberattacks have been targeting critical information infrastructure which is the information systems that store, process and deliver information (Department of Homeland Security, 2011). In 2013, a survey was conducted by Kaspersky Lab and B2B International, indicating that 91% of organisations who took part in the survey had been hit by a cyberattack at least once in a 12-month period, while 9% became victims of cyberattacks (Kaspersky, 2013). Thus, cyberattacks have escalated recently as Choo (2011) emphasises that cyberattacks are increasing in variety and volume. It is important that emphasis is placed on cyberattacks, as anyone possessing a virus infected computer and an internet connection can launch a cyberattack.

This research project is being done to highlight and address security issues, while focusing on cyberattacks on critical information infrastructure. Focus will be placed on a system of controls: preventive, detective and corrective controls, which will be used together to protect the confidentiality, integrity and availability of information. This system of controls is based on the General Systems Theory, which states that a system, within an environment, is made up of elements that are interdependent and contribute to the operation of the whole system (Lin, Duan, Zhao, Da & Xu, 2012). Towards the end of this research project, a model to address insecure critical information infrastructure will be proposed.

1.2 General Area of Research

The general research area for this study is based on cyberattacks on critical information infrastructure. A cyberattack is a criminal act which is committed by using computers in order to damage or disrupt systems and networks (GTAG1, 2005). These cyberattacks occur in cyberspace i.e the internet, where organisations face many cyberthreats (Department of Communications, 2014). Thus, the internet is used as a medium for cyberattacks.

Jordan (2012) explains why the internet was invented: to be used to do research between academic institutions, as well as the US Department of Defence (DOD). Thus it was not designed for security, as its purpose back then was to exchange information between small networks. Due to the emergence of various cyberthreats, security is now essential as information online needs to be protected. Hence, Information Security has been added and aims to protect the confidentiality, integrity and availability of information stored on systems (ISO/IEC 27002, 2005). Figure 1.1 illustrates the CIA Triad Model which depicts the three principles of information: confidentiality, integrity and availability. Confidential information must be protected from being exposed to unauthorized individuals (Whitman & Herbert, 2012). The

integrity of information indicates that information must be complete and not corrupted. Finally, information must only be available to authorized individuals without any interference. These three principles must be maintained in order to effectively secure critical information infrastructure and will be referred to throughout this research project.

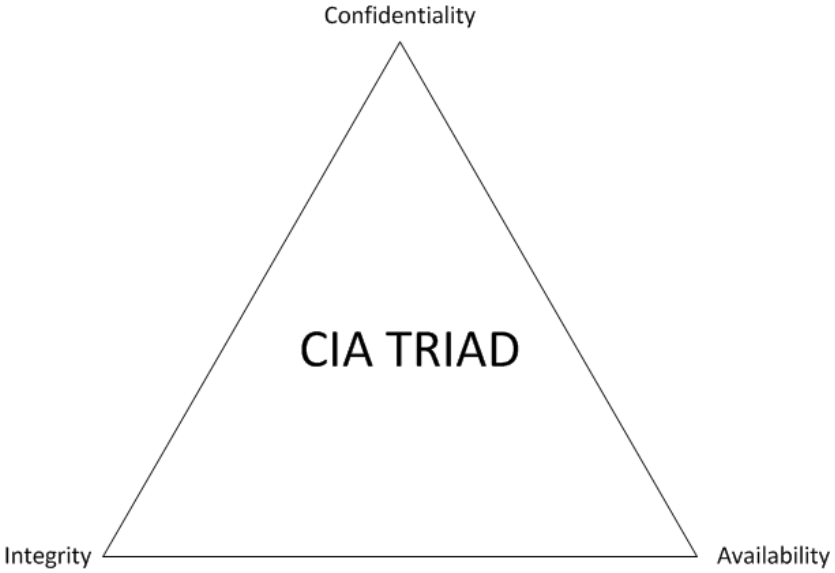

Figure 1.1: CIA Triad Model (ISO/IEC 27002, 2005)

1.3 Problem Statement

Many organisations do not secure their critical information infrastructure effectively and are thus vulnerable to cyberattacks. Vulnerabilities make it easy for cyberthreats to infiltrate or take down critical information infrastructure. Critical information infrastructure is vulnerable as it is connected to the internet, which cyberthreats use as a medium to launch cyberattacks.

1.4 Research Question and Sub-questions

1.4.1 Main Research Question

What security controls can be implemented to effectively secure critical information infrastructure and prevent cyberattacks?

1.4.2 Sub-questions

What types of vulnerabilities may critical information infrastructure possess?

Certain types of vulnerabilities in critical information infrastructure need to be recognized in order to be secured before they are exploited by cyberthreats.

What kinds of cyberthreats create cyberattacks?

Different types of cyberthreats need to be identified. Their impact on critical information infrastructure should be noted in order to protect critical information infrastructure.

What security controls are available to protect critical information infrastructure?

The aim is to identify security controls which are needed to prevent, detect and correct cyberattacks.

1.5 Hypothesis (answering the above sub-questions 1 to 3 respectively)

1. Vulnerabilities such as software vulnerabilities are exploited by cyberthreats and allow these cyberthreats to infiltrate or take down critical information infrastructure.

2. Cyberthreats such as malware create cyberattacks and can steal, damage or make information unavailable to authorized users.

3. Critical information infrastructure needs to be protected from cyberattacks by using security controls, which prevent, detect and correct cyberattacks. Examples of security controls are firewalls, intrusion detection systems and disaster recovery planning.

1.6 Scope of Research

Critical infrastructure is a term which refers to assets that are critical for the operation of a nationôs economy (Department of Communications, 2014). Some examples of critical infrastructure are telecommunications networks, power plants and water supply systems. Cyberattacks which intend to sabotage equipment used in critical infrastructure, such as power plant generators are excluded in this study. Thus, only the information side of critical infrastructure i.e. critical information infrastructure will be discussed. This includes information stored on systems, as well as information delivered via networks such as the internet. In addition, only intentional human attacks on critical information infrastructure will be examined. This includes hackers, disgruntled employees and other entities. Critical information infrastructure disrupted by natural disasters will not be examined.

1.7 Review of Related Literature

Critical information infrastructure is the information systems that store, process and deliver information (Department of Homeland Security, 2011). This information is delivered via networks to users who are connected to the internet.

Despite this, Strickland (2008) emphasises that the internet and the systems connected to it are not very secure, as there are many ways to exploit vulnerabilities in critical information infrastructure. Hence, these vulnerabilities are creating many opportunities for cyberthreats to exploit and consequently steal, corrupt or make information unavailable to authorized users.

Won, Ok-Ran, Chulyun and Jungmin (2011) state that password vulnerabilities are the most common type of vulnerability which is exploited by attackers. Thus, an attacker does not need to find any other vulnerabilities to exploit in order to infiltrate a system. In contrast, Choo (2011) states that naive employees may become victims of phishing scams and consequently submit their passwords on a malicious website created by an attacker. Thus, an attacker does not need to use special software to exploit password vulnerabilities. Alternatively, Jang-Jaccard and Nepal (2014) mention network protocol vulnerabilities such as Domain Name System (DNS) which can be exploited by cyberthreats. This allows an attacker to create a malicious website which is then used to capture confidential information submitted by a user.

Cyberthreats use the internet as a medium to create cyberattacks, as the internet is not effectively monitored and controlled. Knake (2011, p. 6) elaborates on this by stating that ñAs a network of networks, the Internet has no central authority to control itò. The internet is a telecommunications network as it allows parties to communicate with each other over long distances (Telecommunications network, n.d.). These parties include users and organisations that are both connected to the internet. As a result, cyberthreats such as Distributed Denial of Service (DDoS) attacks are capable of taking down websites, thus preventing users from using internet services (Peng, Leckie & Ramamohanarao, 2007). Newman (2006) adds that cyberthreats such as malware are also capable of making information unavailable.

Jang-Jaccard et al. (2014) describe the growing threat of malware by stating that due to the increase in internet speeds and its affordability, more and more users are connecting to it, causing the threat of malware to increase with it. This increase in speed has led to an increase in the amount of data transferred between computers online, known as bandwidth (Bandwidth, n.d.). It is evident that there is a trade-off between the number of internet users and malware. Malware would be stopped if the internet was shutdown, but that is impossible as the internet has been providing beneficial internet services to users.

However, with the variety of cyberthreats which are attacking critical information infrastructure, there are a number of security controls which can be used to protect it. These security controls are put into three categories: preventive, detective and corrective controls (GTAG1, 2005). However, a risk strategy is needed before these three security controls can be implemented (Whitman et al., 2012).

Thus, these three controls must be used together in order to protect critical information infrastructure, including the confidentiality, integrity and availability of information (ISO/IEC 27002, 2005). However these security controls i.e. countermeasures may possess vulnerabilities (Common Criteria, 2005). As a result, security controls which possess vulnerabilities may not function correctly. Hence, critical information infrastructure cannot be completely secure. Flowerday and Von Solms (2007, p. 2), in agreement, state that ñ100% information security is not achievableò.

Thus, it is evident that there is a need to protect critical information infrastructure from cyberattacks, as vulnerabilities in critical information infrastructure are creating opportunities for cyberthreats to exploit and consequently steal, corrupt or make information unavailable to authorized users.

1.8 Research Methodology

This research project was done using secondary data such as articles, journals, books, conference proceedings and news articles. The information retrieved from these resources was categorised into themes, corresponding to various cyberthreats which create cyberattacks. Primary data such as questionnaires and interviews were not used for this research. This project was based on qualitative research and not quantitative research. An extensive literature review was done for this research project using critical thought, when reading various sources of information from different authors. After completing the extended literature review, a model was formulated in order to address the security issues faced by critical information infrastructure. This model implements the General Systems Theory, which was used as the underlying theory of this research project.

CHAPTER 2: VULNERABILITIES POSSESSED BY CRITICAL INFORMATION INFRASTRUCTURE

2.1. Introduction

A vulnerability is a flaw in a system or protection mechanism that exposes a system to cyberattacks (Whitman et al., 2012). An attacker can use cyberthreats to exploit vulnerabilities in order to steal confidential information, damage information or make this information unavailable. As a result, the CIA principles will not be preserved. However, vulnerabilities are not only exploited by external attackers but may also be exploited by disgruntled employees within an organisation. In this chapter software, password, personnel, disaster recovery planning and network protocol vulnerabilities will be discussed in detail.

2.2. The Existence of Vulnerabilities in Critical Information Infrastructure Today

The problem today is that the internet and systems connected to it are not very secure, as there are many ways to exploit vulnerabilities in critical information infrastructure (Strickland, 2008). Hence, these vulnerabilities are creating many opportunities for cyberthreats to exploit and consequently steal, corrupt or make information unavailable. Organisations may not be aware of any vulnerabilities which exist and usually find out when it is too late.

According to Jang-Jaccard et al. (2014) malware was originally created with the purpose of finding security vulnerabilities. However, the irony today is that malware is used to exploit different kinds of vulnerabilities and take advantage of this to launch a malicious attack. The Common Criteria Model will be examined next, including vulnerabilities which are depicted in this model.

2.3 Common Criteria Model

Figure 2.1 shows the Common Criteria Model, which illustrates security concepts and relationships. These security concepts and relationships will be examined before discussing the various types of vulnerabilities which are possessed by critical information infrastructure.

By applying this model to critical information infrastructure, owners refer to organisations who value their assets. These assets represent information which is stored on systems and delivered via networks such as the internet.

On the other hand, threat agents may wish to abuse or damage these assets by stealing confidential information, sabotaging or modifying information or preventing access to

information. Thus, the CIA principles will not be preserved. Examples of threat agents include hackers, disgruntled employees and other entities. These threat agents give rise to threats which target assets. Examples of threats include malware, cybersabotage and Distributed Denial of Service (DDoS) attacks (discussed in chapter 3). Threat agents are often successful in damaging or abusing assets as they exploit vulnerabilities which are present in critical information infrastructure.

However, owners may be aware of vulnerabilities in critical information infrastructure and thus impose countermeasures (i.e. security controls which are discussed in chapter 4) to reduce them. As a result, risks to assets will be reduced. In contrast, countermeasures such as antivirus software may possess vulnerabilities, which will prevent them from identifying and rectifying the latest software vulnerabilities. Software vulnerabilities will be discussed next.

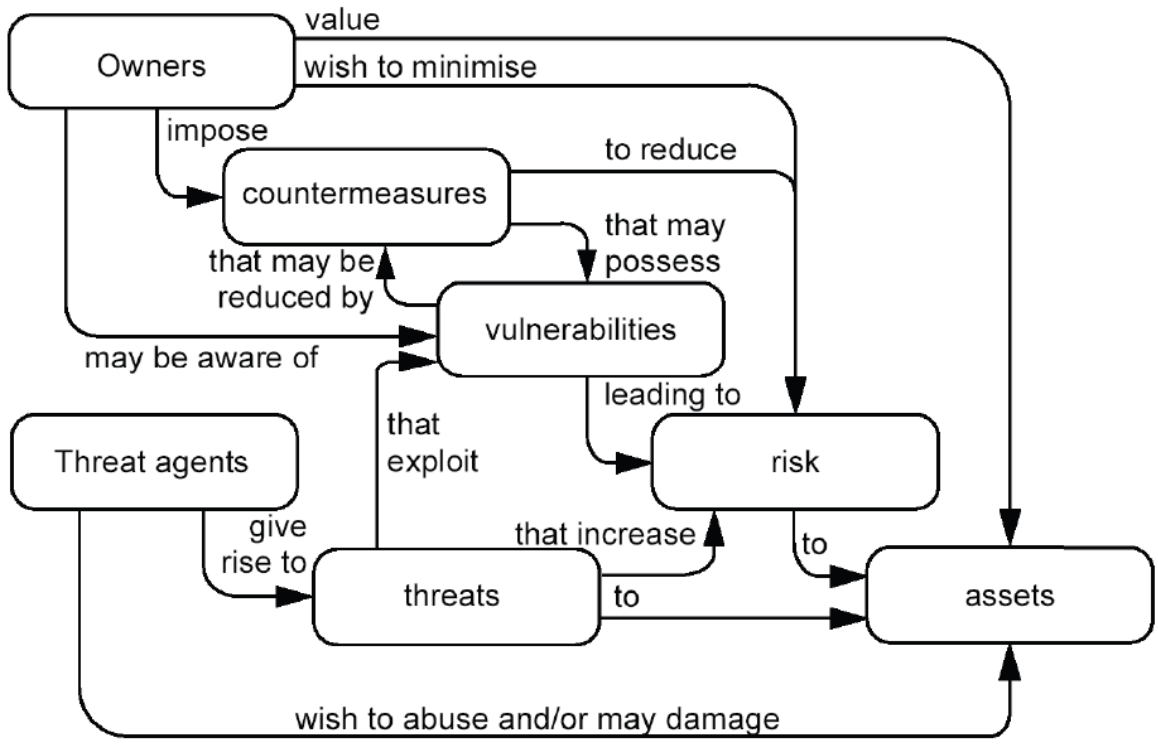

Figure 2.1: Common Criteria Model (Common Criteria, 2005)

2.4 Software Vulnerabilities

A software vulnerability is a flaw in the design of a computer program (Jang-Jaccard et al., 2014). It is these flaws which malware exploit in order to gain unauthorized access to a system. Once access has been gained, the system is at the disposal of the attacker who launches the cyberattack. In contrast, Meunier (2008) states that there is a difference between flaws and vulnerabilities: vulnerabilities are exploitable but flaws are not necessarily exploitable. Although computer programs such as database software can be beneficial for organisations working with large amounts of information, a vulnerability in this software can potentially cause the information stored in the database, to be accessible to the attacker. Two categories of software vulnerabilities: unpatched systems and lack of input validation will be discussed in detail next.

2.4.1 Unpatched Systems

A patch is software which is used to fix any problems which have been found in a software program (Fisher, n.d.). If software running on a system, such as antivirus software, is not regularly patched, attackers will be able to exploit this vulnerability and consequently compromise a system. Despite this, many software programs notify users when new patches are available which can be installed automatically. However, Sood (2009) states that although vendors provide automatic updates, it is up to the user to proceed with the update or not. New patches are released regularly but without a userôs effort to install the patch, it is useless.

Newman (2006) adds that organisations such as Microsoft release a large amount of patches every year. Keeping up with all these patches can overwhelm a user. As a result of this, users may not be consistent when updating their systems, which is crucial since new vulnerabilities arise frequently. If these vulnerabilities are not patched, critical files will be accessible to an attacker and can then be stolen or corrupted.

In contrast, vendors may fail to develop patches in time to address a specific vulnerability. Kirk (2014) refers to an example where a flaw was found in Symantecôs Endpoint Protection software in 2014. Ironically Symantec, an American security company, had not yet developed a patch to fix this flaw which is also known as a zero-day vulnerability. Meunier (2008) defines a zero-day vulnerability as a flaw which is not known to both the public and the vendor. Hence, users and vendors may not know if a cyberthreat has exploited a vulnerability which exists in their software. Kirk also mentions that the zero-day vulnerability was discovered using penetration testing which is discussed in chapter 4 (section 4.4.4). The lack of validation in software is another vulnerability which will be discussed next.

2.4.2 Lack of Input Validation

Input validation is a process which ensures that input data follows certain rules (Jang-Jaccard et al., 2014). Examples of input data are usernames and passwords. Input data which is submitted on websites should be verified to make sure that it meets certain rules. No or incorrect validation will allow attackers to steal confidential information by using SQL injections which exploit the lack of validation. Attackers can enter SQL commands into fields in order to retrieve confidential information from online banking websites. Thus it is important that username and password fields are validated while any commands entered are rejected. Although validation is implemented, password vulnerabilities will still be exploited. Password vulnerabilities will be examined next.

2.5 Password Vulnerabilities

Password vulnerabilities consist of weak passwords and are the most common type of vulnerability which is exploited by attackers (Won et al., 2011). Weak passwords such as an employeeôs name and date of birth can easily get exploited by an attacker. Due to this, an attacker can guess their passwords and gain access to their personal information. By exploiting password vulnerabilities, an attacker does not need to bother finding other vulnerabilities to exploit. Vulnerabilities in an organisationôs personnel will be discussed below.

2.6 Personnel Vulnerabilities

Personnel vulnerabilities comprise of employees who have the potential to damage their organisationôs information (Colwill, 2009). Disgruntled employees have an advantage over external attackers, as most employees have access to confidential information and know where critical systems are located in their organisation. In contrast, external attackers would need to probe a system and look for vulnerabilities to exploit before they can infiltrate a system or network. Disgruntled employeesô use of cybersabotage will be discussed in detail in chapter 3 (section 3.7).

However, personnel vulnerabilities do not only include disgruntled employees. According to Choo (2011) external attackers are able to take advantage of naive employees in order to steal their confidential information. For example, an attacker could send an email to an employee requesting their password in order to keep their email account active. As a result, employees may carelessly give away their passwords. These methods are used in social engineering which is discussed in chapter 3 (section 3.8). Disaster recovery planning vulnerabilities which involves personnel will be examined next.

2.7 Disaster Recovery Planning Vulnerabilities

A disaster recovery plan is a document which specifies the activities that need to be followed, to recover from a disaster (Whitman et al., 2012). However, this plan may contain several vulnerabilities. Due to these vulnerabilities, an organisation may not be able to recover information which has been lost due to a cyberattack. A disaster recovery plan which is not tested regularly in a specific scenario will not be reliable in the event of a disaster (GTAG1, 2005). An example of a scenario could include a DDoS attack which has taken down a website, thus preventing users from accessing their information. Schuchart (2013) mentions another vulnerability involving employees who assume someone else will help the organisation recover after a disaster has occurred. This is the result of an organisation which does not inform its employees about what they can do, to contribute to the disaster recovery plan. In addition, employees may not understand what types of disasters may occur, if the disaster recovery plan does not contain a number of scenarios. The disaster recovery plan is an important security control and will be discussed in chapter 4 (section 4.6.2). Next, vulnerabilities in network protocols will be discussed.

2.8 Network Protocol Vulnerabilities

Network protocols are rules used for communication between computers over the internet (Mitchell, n.d.). An example would be communication over the internet between a user paying taxes online and a government website. Some network protocols are vulnerable to cyberattacks and are exploited in order to disrupt or compromise websites. Peng et al. (2007) mention one vulnerable protocol known as Hypertext Transfer Protocol (HTTP) which is used by websites. The HTTP protocol is exploited by DDoS attacks which are launched to take down websites, thus making information unavailable to users (discussed in Chapter 3 section 3.4).

Jang-Jaccard et al. (2014) explain another vulnerable protocol known as Domain Name System (DNS). The DNS protocol translates website addresses into IP addresses. The HTTP and DNS protocols are both targeted by DDoS attacks. Attackers exploit this protocol which allows them to create malicious websites used to steal confidential information from victims. Hence, it is important that organisations take measures to prevent these protocols from being exploited.

2.9 Conclusion

A number of vulnerabilities in critical information infrastructure were discussed in this chapter. Software vulnerabilities arise due to unpatched systems or website input which has not been validated, while weak passwords are easily exploited by attackers. On the other hand, employees knowingly or unknowingly create vulnerabilities for attackers to exploit. An untested

disaster recovery plan can prevent an organisation from recovering information which has been lost due to a cyberattack. Finally, network protocol vulnerabilities are exploited with the aim of compromising or taking down websites. In chapter 3, a system of controls will be used to address the vulnerabilities which were discussed in this chapter. In the next chapter, a number of cyberthreats which exploit these vulnerabilities will be discussed.

CHAPTER 3: CYBERATTACKS CREATED BY CYBERTHREATS

3.1 Introduction

Many organisations have suffered from cyberattacks that have been created by a variety of cyberthreats. A cyberthreat is a malicious attempt to damage or disrupt a system or network (Cyberthreat, n.d.). Cyberthreats originate from hackers, disgruntled employees or other entities. Various cyberthreats will be discussed in this chapter including: malware, Distributed Denial of Service, cyberwarfare, cyberespionage, cybersabotage and social engineering. In addition, their impact on the CIA principles will be mentioned throughout this chapter. Before these types of cyberthreats are examined, their use of the internet as a medium to launch cyberattacks will be discussed, in order to understand why they are so prevalent.

3.2. The Internet as a Medium Used for Cyberattacks

Cyberthreats use the internet as a medium to create cyberattacks, as the internet is not effectively monitored and controlled. Knake (2011, p. 6) elaborates on this by stating that ñAs a network of networks, the Internet has no central authority to control itò. The internet is a telecommunications network as it allows parties to communicate with each other over long distances (Telecommunications network, n.d.). These parties include both users and organisations that are connected to the internet. As a result, cyberthreats will attempt to disrupt telecommunications networks in order to prevent users from accessing internet services. In addition, cyberthreats will aim to corrupt or steal confidential information stored on organisationsô systems. Malware is capable of doing this and will be discussed in detail next.

3.3 Malware

Malware is software which is used to compromise a system (Won et al., 2011). It includes three categories: viruses, worms and Trojan horses. Malware can be disguised as legitimate software, which organisations may install erroneously, infecting their systems in the process. This could happen due to the use of ineffective security controls which leave a system open to attack.

Davies (2014) refers to an example of a retail business in the USA, known as Target, which became a victim of malware in 2014, despite having a security system in place. This malware was installed on their systems without their knowledge. Although their security system initially detected the malware, Targetôs staff overlooked the alerts. The consequence of this was that the malware intercepted their customersô credit card information which was then stolen during the checkout process. Thus, an organisation may lose its customers due to not having security controls in place or ignoring any warnings.

Rouse (2010b) uses the term cybercrime to describe the example of Targetôs security breach above. Cybercrime refers to the use of computers to engage in illegal activities over the internet. Criminals have taken advantage of the internet by using malware to enable them to steal large amounts of confidential information. It is evident that organisations do not only suffer from the negative impact which malware causes but so do their customers. On top of this, organisations may lose their customers. Thus, effectively securing an organisationôs systems is not only important to an organisation but also its customers.

Praprotnik, Ivanuša and Podbregar (2013) explain how malware can function in the same way as a weapon by attacking systems, ñMalware is basically an offensive weapon, since it is made to attack the desired targetò. This is possible as the ódamageô involves corrupting valuable information provided by internet services or taking down websites belonging to organisations. Strickland (2008) elaborates on this by stating that organisations need to spend a lot of money to repair damages caused by malware. Repairing these damages over a long period is very expensive and it would be more cost efficient to spend money on security controls, instead of spending money every time information stored on a system gets damaged.

Jang-Jaccard et al. (2014) describe the growing threat of malware by stating that due to the increase in internet speeds and its affordability, more and more users are connecting to it, causing the threat of malware to increase with it. This increase in speed has led to an increase in the amount of data transferred between computers online and is known as bandwidth (Bandwidth, n.d.). It is evident that there is a trade-off between the number of internet users and malware. Malware would be stopped if the internet was shutdown, but that is impossible as the internet has been providing beneficial internet services to users. Viruses which are a specific type of malware will be examined next.

3.3.1 Viruses

A virus is a program written by a hacker, which attaches itself onto other programs and spreads when it is moved to different computers (Won et al., 2011). A common method used by a virus to spread is by making copies of itself. As a result, viruses are capable of corrupting and stealing confidential information from organisations on a large scale. Due to the affordability of storage media such as flash drives, it is very easy for these viruses to rapidly spread.

Finkle (2014) refers to a virus named ñBackoffò which attacked point-of-sales systems belonging to organisations in the USA, in 2014. This virus was used by cybercriminals to steal payment-

card details and was undetectable by most types of antivirus software, making it an even bigger threat. Worms, which are another type of malware, will be discussed below.

3.3.2 Worms

Worms are a specific type of malware which steal confidential information from a system, as well as damage and disrupt it. Unlike viruses, worms make additional copies of themselves and spread from one computer to the next in a network, without needing people to move the infected files around (Won et al., 2011). Hence, they can spread faster than viruses, as they infect many systems independently. Goel (2011) states that one purpose of worms is to create a botnet, used to launch DDoS attacks. Thus, it is evident that worms are also able to create opportunities for other cyberthreats to attack.

Bell (2014) refers to an example of a worm nicknamed Conficker, which exploited a number of vulnerabilities in Microsoftôs old operating system, Windows XP. Although Microsoft continuously warned organisations to upgrade their systems to the latest version of Windows, many organisations ignored the warning and still continued to use Windows XP. Attackers have seen this as an opportunity and have been able to exploit several vulnerabilities in Windows XP, in order to gain unauthorized access to organisationsô systems. A Trojan horse, the third category of malware, will be examined next.

3.3.3 Trojan Horse

A Trojan horse (or Trojan) is a type of malware which disguises itself as legitimate software, while it is actually used for malicious purposes (Newman, 2006). Once the Trojan horse is installed by an unsuspecting user, it is able to attack a system by corrupting or stealing information. On top of this, an installed Trojan allows an attacker to remotely control the infected computer. Although Trojan horses cannot make copies of themselves, Jang-Jaccard et al. (2014) state that Trojan horses are the most common type of malware. This is due to many users who download software programs infected with a Trojan horse, or click on malicious links in an email. Jones (2005) refers to a past event involving the UKôs government departments and businesses which were attacked by Trojan horses, in 2005. Hackers sent emails containing a Trojan horse to these organisations, resulting in the theft of economic information. Computers infected with Trojans are used in DDoS attacks and will be discussed below.

3.4 Distributed Denial of Service

Distributed Denial of Service is an attack which uses a group of infected computers to take down a website, by flooding it with unnecessary traffic (Praprotnik et al., 2013). This group of infected computers is known as a botnet while an infected computer is known as a zombie. The infected computers belong to innocent people who may have become infected due to clicking on a malicious link in an email or downloading free software (which is disguised as a Trojan horse). These zombie computers are capable of infecting other computers over the internet and are controlled remotely by attackers. Jenik (2009) refers to a past event where Estonia, a very connected country online, was a victim of DDoS attacks in 2007. Estonia depends a lot on internet services such as online banking and due to DDoS attacks its internet services were brought down. This resulted in users who were not able to access their online banking accounts and thus could not make any transactions.

Another definition of DDoS is defined by Meunier (2008), who states that, ñdenial of service is the consequence of an attack and not an attack scenarioò. Malware is able to attack computers by infecting them, causing these zombie computers to launch DDoS attacks. Thus, attackers can use a combination of cyberthreats to launch cyberattacks on a large scale.

Won et al. (2011) explain the process of a DDoS attack. First of all, all of the infected computers simultaneously send a request to a targeted website via a command from an attacker. The target is then forced to reply to the requests made by the zombie computers and due to the large amount of traffic generated, may not be able to cope and thus shutdown. The attacker is hard to identify as their IP address is spoofed as the infected computersô IP address. Although it is difficult to identify the attacker, it is possible to know when a DDoS attack has taken place if the targeted website has slowed down significantly.

Everett (2009) adds that anyone can rent or buy a botnet from a cybercriminal, for a certain price. A program with a user-friendly interface is provided to control the botnet. This allows even the novice user to launch cyberattacks by using the botnet to send phishing emails, thus stealing confidential information from users. This is another reason why there has been a large increase in the number of cyberattacks as botnets are easily available. DDoS attacks are used extensively in cyberwarfare which will be examined below.

3.5 Cyberwarfare

Cyberwarfare is defined as conflict which occurs over the internet and involves politically motivated attacks which target information systems and are conducted by governments or hackers (Rouse, 2010a). These attacks are capable of taking down government websites, thus preventing citizens from communicating with their government online via e-government. Anyone with a computer and an internet connection can take part in cyberwarfare intentionally or unintentionally if their computer is turned into a zombie computer.

Goelôs (2011) view is that governments do not directly launch cyberattacks but instead support and sponsor hacker groups to carry out these attacks. An example of this is mentioned by Rouse (2010a); in 2007, the USAôs military agencies were hacked into by unknown attackers, who managed to download terabytes of information. The anonymity provided by the internet allowed these hackers to hide their identities. This has made it hard for organisations that have been attacked to identify their attackers.

Praprotnik et al. (2013) compare cyberwarfare to traditional warfare which requires a lot of resources such as personnel and weapons. In contrast, cyberwarfare only requires knowledge and a computer to engage in online conflict. Taking part in cyberwarfare is also safer for personnel who would normally risk their lives on the battlefield (Denning & Denning, 2010). Many countries are taking advantage of this by infiltrating insecure critical information infrastructure belonging to other countries. Ironically a country which launches cyberattacks on another country may also have insecure critical information infrastructure. Rapoza (2013) refers to an example where China, which has launched many cyberattacks in the past, was a victim of a cyberattack; in 2013, the US government hacked into Chinese mobile phone companies and stole confidential information such as text messages. Thus it is evident that even attackers are open to cyberattacks due to their insecure critical information infrastructure. Cyberespionage, which is another area of cyberwarfare, is discussed next.

3.6 Cyberespionage

Cyberespionage involves the use of computers to steal confidential information from systems (Praprotnik et al., 2013). Governments also take part in cyberespionage by stealing confidential information from other governments. Everett (2009) elaborates on this by stating that a developing nation may use cyberespionage in order to catch up with first world nations. Alternatively, an organisation may plan to steal trade secrets from another organisation and use it to improve their competitive advantage in their industry.

Cyberespionage helps government spies, on intelligence operations, to remotely steal files from other governments (Denning et al., 2010). As a result of this, many governments are starting to engage in cyberespionage due to its convenience, as spying can take place in front of a computer.

On the other hand, Bradbury (2013) explains how individuals with minimal computer knowledge are able to view confidential information of governments on WikiLeaks. It is evident that cyberespionage does not only involve governments and hackers, but also inexperienced individuals who possess a computer and an internet connection. Cybersabotage is another cyberthreat which will be discussed next.

3.7 Cybersabotage

Cybersabotage is an attack conducted by an individual or organisation, with the aim of damaging information, defacing or taking down websites (Goel, 2011). As a result, cybersabotage is used to deny access to information using methods such as DDoS attacks. The modification of information illegally to reflect inaccurate information is also part of cybersabotage (Newman, 2006). For example, an attacker may decide to alter the tax amounts that users owe to the government. Hence, users will view the wrong information when paying taxes online.

On the other hand, Finnan (2014) mentions that hacktivists sabotage websites by defacing them or use DDoS attacks to protest against some cause. He refers to a past event where hacktivists attacked various Kenyan government websites using DDoS attacks, in 2014. Hacktivists launched these attacks in anger of corruption in the country. Government websites which were sabotaged included the Kenya Defence Force website. Thus it is evident that the motive of some cyberattacks is to raise awareness on a specific matter.

James (2012) adds that there is another source of cybersabotage which involves disgruntled employees. Disgruntled employees often sabotage their organisationôs information as an act of anger due to reasons such as receiving low salaries or being shown no respect from their employer. These employees can damage their organisationôs reputation by defacing their organisationôs websites or corrupting information belonging to their organisation. Although organisations need to focus on external threats such as malware, equal focus must be placed on internal threats such as disgruntled employees. Even though a security control such as a firewall is preventing outside intruders from accessing an organisationôs system, it only takes one disgruntled employee to sabotage the information stored on these systems, which a firewall cannot prevent. However, an employee may unintentionally create an opportunity for their organisation to be attacked. This will be discussed next, under the topic of social engineering.

3.8 Social Engineering

Social engineering is a method used by attackers to deceive employees into giving them their confidential information (Newman, 2006). Even if an organisation secures its systems effectively, employees who are easily tricked will unknowingly let malware enter their system. Malware will enter the system if preventive controls such as antivirus software do not exist. There are various types of methods used in social engineering such as phishing and baiting. Phishing is used a lot in social engineering and will be discussed next.

3.8.1 Phishing

According to Jang-Jaccard et al. (2014) phishing is a method which is used to obtain confidential information from innocent people, by masquerading as a trustworthy source. These innocent people may receive an email from an attacker requesting their passwords for a certain reason. The victim then clicks a link in the email which directs them to a malicious website belonging to the attacker. Any information entered onto this website is sent to the attacker. Guerrini (2014) refers to a past event where hacktivists protested against the large amounts of money spent on Brazilôs World Cup, in 2014. They went on to send phishing emails to employees of the Ministry of Foreign Affairs in Brazil, requesting them to fill in their credentials on a fake website. The hacktivists then used these credentials to access the employeesô emails and consequently stole their messages and contacts. On top to this, the contacts of these employees would eventually receive these phishing emails and their credentials could also be compromised, which shows how fast phishing emails spread.

Won et al. (2010) add that hackers use botnets to send excessive amounts of phishing emails. Thus, botnets are not only used to launch DDoS attacks as discussed earlier on. Using botnets makes it easy to send phishing emails to every single employee in an organisation, as opposed to the hacker using their own computer to send the phishing emails. It is important for organisations to be aware of both phishing and DDoS, as both of these cyberthreats use botnets to launch cyberattacks. Another method used in social engineering known as baiting is examined below.

3.8.2 Baiting

Baiting involves an attacker who leaves a malware infected storage media such as a flash drive in an area, where it can easily be found by the targeted victim (Krombholz, Hobel, Huber & Weippl, 2013). This flash drive could have a label such as ñconfidentialò to tempt the victim to take a look at its content on their computer. For example, the flash drive could be dropped on an organisationôs premises by an attacker targeting a specific employee. The employee may then

insert the flash drive into their computer. As a result, the malware will get installed on the computer, allowing the attacker to remotely control it. Hence, the organisationôs computer may end up being used to launch a DDoS attack on another organisation.

3.9 Conclusion

Cyberthreats use the internet as a medium to attack organisations with insecure critical information infrastructure. Many of these cyberthreats have the same intention which is to steal, corrupt or make information unavailable to authorized users. In this chapter, various cyberthreats were discussed including malware, Distributed Denial of Service, cyberwarfare, cyberespionage, cybersabotage and social engineering. Examples of organisations which were attacked by cyberthreats in the past were also discussed. In the next chapter, security controls used to counter these cyberthreats will be examined.

CHAPTER 4: SECURITY CONTROLS USED TO PROTECT CRITICAL INFORMATION INFRASTRUCTURE

4.1 Introduction

With the variety of cyberthreats which are attacking critical information infrastructure, there are a number of security controls that can be used to protect it. Security controls are countermeasures which are used to avoid, counteract or reduce security risks (Northcutt, n.d.). These security controls are put into three categories: preventive, detective and corrective controls. These three security controls will be examined in this chapter, along with risk strategies which are needed to implement them. Next, the classifications of controls will be discussed.

4.2 Classifications of Controls

Figure 4.1 shows some control classifications. General controls comprise of access controls and disaster recovery plans. Governance controls consist of policies while management controls include separation of duties. On the other hand, technical controls include antivirus software and firewalls. Application controls are not included in this research project.

The controls mentioned above can be put into three categories: preventive, detective and corrective controls. Preventive controls prevent security incidents from happening. An organisation should have more preventive controls compared to detective and corrective controls, as preventing a cyberthreat from attacking a system or network is the best defence. Detective controls detect any security incidents that have avoided preventive controls. Lastly, corrective controls correct incidents that have been detected. Both technical and non-technical controls will be discussed in this chapter. Next, the application of the General Systems Theory to these three controls will be discussed.

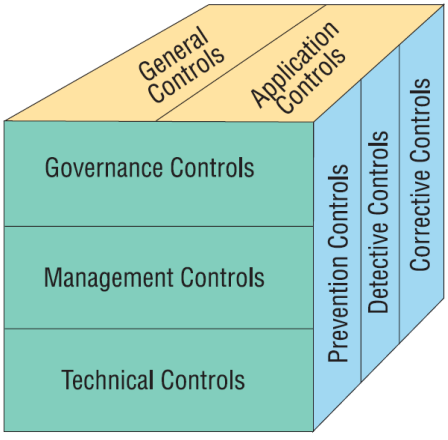

Figure 4.1: Some Control Classifications (GTAG1, 2005)

4.3 Application of General Systems Theory to System of Controls

The General Systems Theory states that a system, within an environment, is made up of elements which are interdependent and contribute to the operation of the whole system (Lin et al., 2012). In this instance, preventive, detective and corrective controls are the three elements which form a system of controls (GTAG1, 2005). Thus, these three controls must be used together in order to protect critical information infrastructure, including the confidentiality, integrity and availability of information. However, there may be vulnerabilities in these three controls which will make them ineffective. For example, preventive controls such as antivirus software may have software vulnerabilities. Any vulnerabilities found will be exploited by a cyberthreat, which will allow the cyberthreat to bypass antivirus software. Thus, critical information infrastructure cannot be completely secure. Flowerday et al. (2007, p. 2), in agreement, state that ñ100% information security is not achievableò.

If two controls are implemented but one is missing, critical information infrastructure will still be vulnerable to cyberattacks. For example, if detective controls are missing and a cyberthreat manages to bypass preventive controls, it will not be detected. However, using all three controls together will help to increase the level of security in critical information infrastructure.

Whitman et al. (2012) mention a military strategy known as defence-in-depth, which is the use of multiple layers of security controls. Using this strategy will increase the level of security in an organisation, since multiple security controls are used. Defence-in-depth is related to the General Systems Theory as preventive, detective and corrective controls are all used together as a ówholeô in this strategy. Preventive controls, which are the first line of defence, will be discussed next.

4.4 Preventive Controls

Preventive controls are used to prevent cyberattacks from attacking a system (Peng et al., 2007). Most cyberattacks which are launched use spoofed IP addresses to hide the true origin of the attack. These preventive controls are used to ensure that cyberattacks do not gain unauthorized access to a system or network. Before preventive controls are implemented, the defend strategy (a risk strategy) needs to be selected. The defend strategy attempts to prevent the exploitation of vulnerabilities (Whitman et al., 2012). This is achieved by implementing preventive controls such as policies which will be examined next.

4.4.1 Policies

Policies are rules which are set by the board of directors and executive management of an organisation (GTAG1, 2005). Policies are implemented to help increase security in an organisation. Some policies which could be implemented include allowing people to only access specific information based on their role. For example, an ordinary employee should not be allowed to access confidential information such as trade secrets. In addition, policies should be set to ensure that strong passwords are used and that passwords are updated regularly in an organisation.

All preventive, detective and corrective controls should comply with policies applied by management. For instance, a firewall should be configured by an IT employee to comply with policies, stating what type of traffic should be allowed to pass through and what should be blocked. A firewall is another preventive control and will be discussed below.

4.4.2 Firewalls

A firewall is a security control which is used to manage incoming and outgoing network traffic and determines if the traffic should be allowed through based on certain rules (Jang-Jaccard et al., 2014). For example, traffic coming from outside an organisationôs network is analysed by the firewall to check if it meets certain rules specified by the firewall. If it does not meet any of these rules, the firewall will prevent the traffic from entering the network. A firewall is useful as it allows organisations to define their own firewall rules.

However, Arbor Networks (2012) highlight an issue with firewalls; firewalls are vulnerable to DDoS attacks and on top of this, are not able stop these attacks. This is due to a large number of open ports on a firewall which can be exploited. Thus, even if a certain port is blocked on the firewall, an attacker can use another port to infiltrate a system or network. Peng et al. (2007) elaborate on this by stating that one of these open ports is used by the HTTP protocol. Firewalls allow HTTP traffic generated by users using internet services to enter the network. However, HTTP traffic is also generated by botnets, thus firewalls will not be able to block this traffic. Since attackers controlling botnets use the IP addresses of zombie computers, a firewall will not be able to determine if traffic passing by is legitimate. Thus, implementing a firewall as the only security control is insufficient. Other security controls should also be implemented to compensate for these disadvantages. Another type of preventive control which also manages traffic is an intrusion prevention system and is discussed next.

4.4.3 Intrusion Prevention Systems

An intrusion prevention system (IPS) is a security control which is able to prevent cyberthreats from entering a system or network, as well as detect cyberthreats which have been found on a system or network (Whitman et al., 2012). Hence, an intrusion prevention system acts as both a preventive and detective control. Won et al. (2011) mention two methods used by intrusion prevention systems; the first method used is known as signature-based detection (also used by antivirus software), where signature definitions are checked to see if incoming traffic matches any known signatures. If a match has been found, the intrusion prevention system will prevent the traffic from entering the system or network. The second method is anomaly-based detection which an intrusion prevention system uses to monitor traffic as it occurs and compares it to ónormalô traffic, based on statistics which are stored over time. If abnormal traffic is detected, the intrusion prevention system will alert the user and the traffic will be prevented from entering the system or network. Anomaly-based detection is useful as an alternative method, in the event that signature-based detection misses detecting any malicious traffic.

Unfortunately, there are a number of disadvantages which intrusion prevention systems possess. According to Arbor Networks (2012), intrusion prevention systems may miss new cyberthreats due to signature definitions not being updated. This is a problem as new cyberthreats are frequently being developed by attackers. Thus it may be difficult to continuously update signature definitions. Intrusion prevention systems are also not able to stop DDoS attacks and are targeted first by these attacks, which firewalls also experience as mentioned early on. Due to this disadvantage, an organisation cannot rely on this control as the only layer of defence. Hassell (2005) mentions another disadvantage which the possibility of false alarms being raised by an intrusion prevention system. This is an issue as large amounts of traffic may not necessarily be malicious. For instance, an employee could be downloading a large file over the organisationôs network. This could be seen as abnormal behaviour by an intrusion prevention system. Penetration testing, another preventive control used to test security controls, will be discussed next.

4.4.4 Penetration Testing

Penetration testing is a set of security tests that simulate attacks made by an external attacker (Whitman et al., 2012). These security tests are done in order to identify any vulnerabilities in a system or network. These vulnerabilities can then be secured once they have been found. Hence, penetration testing is a preventive control as once vulnerabilities have been identified and secured, cyberthreats will be prevented from entering a system or network. A penetration tester

may be hired by an organisation to run the tests (Northcutt, Shenk, Shackleford, Rosenberg, Siles & Mancini, 2006). However, a penetration tester does not damage or steal an organisationôs confidential information and would need permission to run a penetration test. In contrast, Brewster (2014) states that in the United Kingdom scanning for vulnerabilities using penetration testing is punishable. Thus it is important that permission is granted to conduct penetration testing, as without permission a penetration test will be seen as another malicious cyberattack.

Penetration testing also involves exploiting personnel vulnerabilities via social engineering, by focusing on the human element. This form of penetration testing is done without the motive of stealing confidential information such as usernames and passwords. Solomon (2014) refers to an event where a Canadian organisation used penetration testing by sending phishing emails to its employees. Many of the employees ended up being tricked into clicking the link in the phishing email and consequently gave away their credentials. Employees can be given security training to raise awareness on phishing scams, in order to prevent them from being tricked again. Penetration testing is also used to test the security of other security controls such as firewalls, which ensures that only legitimate traffic is allowed to pass through the firewall (Everett, 2009). Once different vulnerabilities have been identified, they can be secured by using other controls such installing the latest patches.

However, a drawback of penetration testing is that it might not find all the vulnerabilities in a system or network, as new vulnerabilities emerge over time (Northcutt et al., 2006). After the penetration test has been conducted, a report is generated which clearly shows the results including any vulnerabilities which were detected on the system or network. Employees can look at the report and then decide what action should be taken to secure these vulnerabilities. Antivirus software, which is another preventive control, will be discussed next.

4.4.5 Antivirus Software

Antivirus software is not only a preventive control but also a detective and corrective control (Northcutt, n.d.). It acts as a preventive control by preventing malware from attacking a system, which may steal confidential information or corrupt it. For example, if a user inserts an infected flash drive into a computer, the antivirus software will alert the user that malware has been found on the flash drive. As a result, the antivirus software will remove the malware before it attacks the system. It is important that antivirus software is updated regularly to protect systems from the latest malware. Patches, which are used to update antivirus software and other programs, will be examined below.

4.4.6 Patches

A patch is software which is used to update or fix a programôs problems (Fisher, n.d.). Besides fixing these problems, its major use is to address software vulnerabilities. Once a patch has been applied to an unpatched system, vulnerabilities will be secured. Thus, cyberthreats will be prevented from entering a system. Won et al. (2010) mention an example where vendors provide updates to prevent zombie computers from exploiting software vulnerabilities. Most software programs allow patches to be updated automatically, but it is up to the user to select this setting. It is important that updates are installed automatically, as employees may forget to do so manually. Anti-social engineering techniques used to counter phishing (which was discussed in chapter 3 section 3.8.1), will be discussed next.

4.4.7 Anti-social Engineering Techniques

There are different techniques which can help prevent employees from becoming victims of social engineering scams such as phishing. Twitchell (2006) mentions an example such as providing security training to employees in order to raise awareness on phishing methods used by attackers. Policies can also be implemented such as ensuring that the latest internet browser updates are installed regularly. This will help internet browsers to identify any malicious signs on a website and warn employees beforehand. Won et al. (2011) elaborate by stating that internet browsers display pop-up windows, warning users of any suspicious signs which have been detected on a website. Despite this, employees may overlook these warnings. As a result, they may enter their credentials on a malicious website although they were warned in advance. The second layer of security: detective controls will be discussed in detail below.

4.5 Detective Controls

Detective controls are used to detect cyberthreats which have been found on a system or network (Peng et al., 2007). If a cyberthreat has been able to bypass preventive controls then detective controls would ensure that the cyberthreat is identified. The mitigation strategy, which is another type of risk strategy, would need to be selected before implementing detective controls (Whitman et al., 2012). This strategy aims to reduce the impact caused by the exploitation of a vulnerability, which has allowed a cyberthreat to infiltrate a system or network. The mitigation strategy is important as it ensures that attacks are detected early. A number of detective controls will be examined next.

4.5.1 Antivirus Software

Antivirus software functions as a detective control by alerting a user when malware has been found on a system (Northcutt, n.d.). An example of this would be a message which appears, warning a user that a threat has been detected e.g. after a flash drive has been plugged into a system.

Won et al. (2011) explain how antivirus software finds malware by using two different methods. The first and most common method is to check for viruses on a system, while comparing anything found to a list of virus signatures (these are known viruses which are stored in a database). The second method is to find malware based on unusual changes in the behaviour of a system. For example, the speed of a system could randomly slow down, delaying access to information. In contrast, Praprotnik et al. (2013) mention that some attackers are capable of altering virus signatures. As a result, this will allow malware to avoid detection by antivirus software. Attackers controlling botnets use this technique which makes it difficult to remove malware from zombie computers. The methods of detection used by antivirus software are also used by intrusion detection systems. Intrusion detections systems will be discussed next.

4.5.2 Intrusion Detection Systems

An intrusion detection system (IDS) is a security control which is used to detect cyberthreats and alert an administrator if any are found on a system or network (Jang-Jaccard et al., 2014). However, intrusion detection systems can only detect cyberthreats and not prevent them. Thus, using an intrusion prevention system is more effective than using an intrusion detection system. Intrusion detection systems are able to detect malicious traffic which may be overlooked by firewalls. Intrusion detection systems use the same methods of detection as intrusion prevention systems and experience similar disadvantages as explained earlier on.

Goel (2011) refers to a past event involving intrusion detection systems. In 2009, a group of hackers infiltrated the network of various organisations in the United States. They were able to do this successfully as they disabled the intrusion detection systems used by these organisations. As a result of this, their intrusion was not detected and they were able to steal credit card information from the organisationsô systems. Hence, it is crucial that organisations do not only rely on intrusion detection systems to protect their confidential information. In the next section, another type of intrusion detection system known as a honeypot will be discussed.

4.5.3 Honeypots

A honeypot is a decoy system which is setup to gather information about an attackerôs activities by luring the attacker into the honeypot (Whitman et al., 2012). It is added to an organisation as an extra system and lures attackers away from critical systems. The activities performed by the attacker on the honeypot are recorded in a log and can help an organisation to prosecute the attacker. Hunter and Irwin (2011) add that a honeypot is designed to run vulnerable services which an attacker can exploit in order to gain access to the honeypot. An attacker may choose to infect the honeypot with malware which can then be analyzed. Using a honeypot solves the problem of having to distinguish between legitimate and illegitimate traffic (a problem which the traditional intrusion detection system has). As a result, organisations can understand different attack methodologies and protect themselves from future attacks.

Jang-Jaccard et al. (2014) mention that honeypots can also be used to analyze botnets in order to find ways to counter them. Fortunately, there will be no confidential information stored on the honeypot for the attacker to steal or destroy. On the downside, Won et al. (2010) state that due to the popularity of honeypots today, attackers have found ways to prevent them from falling into these traps. The irony is that although honeypots are made to detect attacks, tools are available to detect these honeypots such as ñSend-Safe Honeypot Hunterò. Thus, if attackers use this tool, they will avoid honeypots. Thus, the logs used to store the attackersô activities will be empty. Corrective controls, which are the third and final layer of security, will be discussed next.

4.6. Corrective Controls

Corrective controls are used to remove any cyberthreats present in the system, as well as reduce or recover from any damage caused by these cyberthreats (Peng et al., 2007). Corrective controls are used once a cyberthreat has managed to bypass preventative controls and evade detective controls. The mitigation strategy would need to be used to implement corrective controls, which will respond to an attack as soon as possible (Whitman et al., 2012). A number of corrective controls will be examined in the remainder of this chapter.

4.6.1 Antivirus Software

Antivirus acts as a corrective control by removing any malware which has been found on a system (Won et al., 2011). This malware could have damaged or stolen confidential information from a system. Although antivirus software can remove malware that has infected a system, it is not able to recover information which may have been corrupted. A disaster recovery plan can address this issue and will be discussed next.

4.6.2 Disaster Recovery Plan

A disaster recovery plan is a document which specifies the activities that need to be followed to recover from a disaster (Whitman et al., 2012). The disaster which is discussed in this research project refers to information which has been stolen and corrupted due to cyberthreats such as malware or made unavailable due to DDoS attacks.

Musthaler (2013) explains that a disaster recovery plan can contain methods to mitigate DDoS attacks, thus an organisation can respond quickly to these attacks. In the event that a DDoS attack takes down an online banking website, an organisation can follow methods in the disaster recovery plan to get the website up as soon as possible. If there are no methods in the plan which explain how to respond to a DDoS attack, the online banking website will stay offline and customers will not be able to make online transactions. Thus, this will negatively affect an organisationôs reputation as customers will be unhappy.

Whitman et al. (2012) mention another element of a disaster recovery plan which is backups. Backing up information is an important part of this plan and should be done on a regular basis, as organisations store large amounts of information on their systems. Thus, a disaster recovery plan acts as a corrective control since information which has been corrupted can be recovered from backups. As a result, information which is provided by systems will now be available to both employees and customers. In the next section, patches as a corrective control will be discussed.

4.6.3 Patches

Patches do not only function as a preventive control but are also used as a corrective control, as they fix flaws which have been found in software programs (Fisher, n.d.). The vulnerability which a cyberthreat may have exploited is patched so that the same vulnerability cannot be exploited in the future. However, new vulnerabilities may be discovered, thus the latest patches should be regularly applied when available. Another corrective control called a Zombie Zapper will be examined next.

4.6.4 Zombie Zapper

Zombie Zapper is a free tool which is used as a corrective control. It can be used to command a zombie computer to stop flooding a website with traffic (Jenik, 2009). This will help organisations to save money instead of looking for some other commercial tool to stop DDoS attacks. Jayawal, Yurcik and Doss (2002) add that the Zombie Zapper tool works by imitating the attacker who is controlling the botnet. The zombie computers are tricked into thinking that the command is given by the attacker, while it is actually the Zombie Zapper tool which is

issuing the command. An organisation which is using an intrusion detection system can also set it to automatically run Zombie Zapper.

4.7 Conclusion

A system of controls compromising of preventive, detective and corrective controls was discussed in this chapter. The General Systems Theory was also discussed, along with the concept of defence-in-depth which emphasises the use of all three controls. Before security controls are implemented, a risk strategy needs to be selected. The defend strategy is selected to implement preventive controls such as firewalls, which prevent cyberthreats from entering a system or network. On the other hand, the mitigation strategy is used to implement detective controls such as intrusion detection systems, which detect cyberthreats that have bypassed preventive controls. Once these cyberthreats have been detected, a corrective control such as antivirus software is used to remove them, while a disaster recovery plan can help an organisation to recover its information in the event of a disaster. The mitigation strategy is used to implement these corrective controls. It is important that organisations do not only use one of these controls as the only layer of security, but should use other controls as well. In the next chapter, a model will be formulated to address insecure critical information infrastructure.

CHAPTER 5: PROPOSED MODEL

5.1 Introduction

In this chapter, a model is proposed to address insecure critical information infrastructure and will thus address the research problem. This model was formulated as a result of an extensive literature review which covered chapters 2, 3 and 4. The General Systems Theory will be applied to the proposed model in order to examine how the elements of the system work together as a ówholeô. Next, the proposed model will be examined, including its elements and relationships.

5.2 Model to Address Insecure Critical Information Infrastructure

In Figure 5.1, cyberthreats exploit vulnerabilities in critical information infrastructure in order to infiltrate or disrupt it. Cyberthreats do this with the aim of stealing, corrupting or making information unavailable to users. To counter these cyberthreats, risk strategies are needed to implement specific security controls. The risk strategies depicted in this model are the defend strategy and mitigation strategy. The defend strategy is used to prevent the exploitation of vulnerabilities in critical information infrastructure, while the mitigation strategy is used to reduce the impact caused by the exploitation of vulnerabilities. The defend strategy is used to implement preventive controls, while the mitigation strategy is used to implement detective and corrective controls. Once risk strategies have been selected and security controls have been implemented, they will ensure that the confidentiality, integrity and availability of information are ensured. As a result, risks to information will be reduced which includes the theft, modification or corruption of information, as well as the unavailability of information. Thus, this model will address insecure critical information infrastructure.

The proposed model is a differentiated model that uses certain elements from the Common Criteria Model (Common Criteria, 2005) and the CIA Triad Model (ISO/IEC 27002, 2005). These two models are both general models (Olivier, 2009). The original CIA Triad Model does not illustrate any elements that show how the confidentiality, integrity and availability of information are preserved. On the other hand, the proposed model illustrates how risk strategies and security controls can be used to ensure that the CIA principles are preserved. In the next section, the General Systems Theory will be applied to the proposed model and will be discussed in detail.

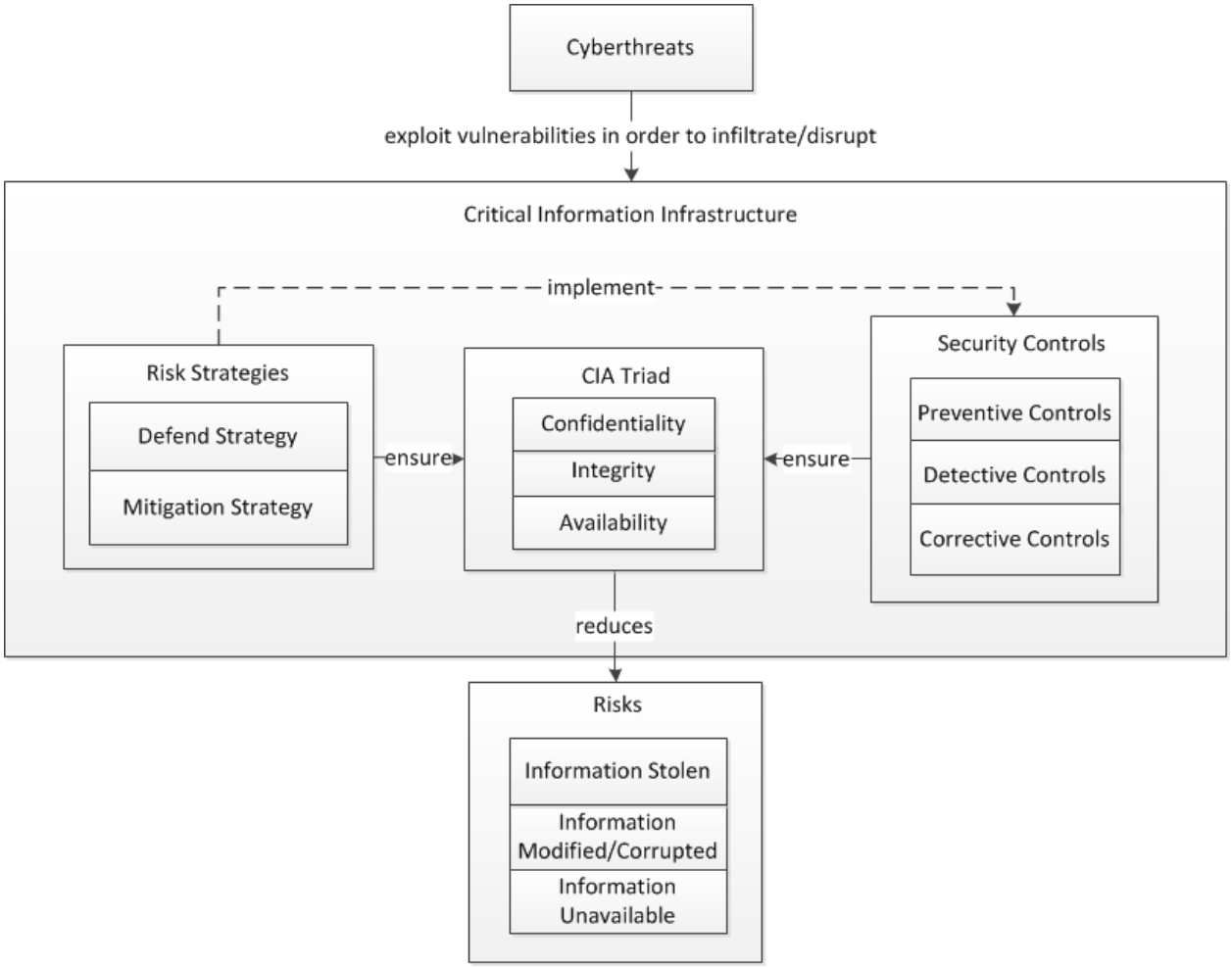

Figure 5.1: Model to Address Insecure Critical Information Infrastructure

5.3 Application of General Systems Theory to Proposed Model

The General Systems Theory states that a system, within an environment, is made up of elements which are interdependent and contribute to the operation of the whole system (Lin et al., 2012). This system has inputs which are processed into outputs.

By applying the General Systems Theory to the proposed model, critical information infrastructure is the overall system and is made up of three elements (i.e. sub-systems) which contribute to the functioning of the overall system. These three sub-systems are: risk strategies, the CIA Triad and security controls (system of controls). Each sub-system is further broken down into its elements. Thus, the General Systems Theory is hierarchical as it has different levels.

The first sub-system, risk strategies, is made up of the defend strategy and mitigation strategy elements. Both of these strategies are needed to implement all three controls.

The second sub-system is the CIA Triad and is made up of three elements: confidentiality, integrity and availability. The CIA Triad can only be made a ówholeô with all three elements.

The third sub-system is security controls. This sub-system is made up of preventive, detective and corrective controls. If preventive, detective or corrective controls are missing, critical information infrastructure will be vulnerable to cyberattacks. For instance, if a cyberthreat bypasses preventive controls and detective controls are missing, it will not be detected. Thus, all three controls are needed to form a system of controls.

Hence, if any elements of the three sub-systems are excluded, then the output (reduced risks) will not be achieved. These three sub-systems (and their elements) are used as input, while the process consists of selecting a specific risk strategy to implement security controls.

5.4 Conclusion

In this chapter, a model to address insecure critical information infrastructure was proposed. The proposed model, including its elements and relationships were discussed in detail. It illustrates how risk strategies can be used to implement security controls, which consequently ensures that the confidentiality, integrity and availability of information are preserved. As a result, risks are reduced and insecure critical information infrastructure has been addressed, which solves the research problem. The General Systems Theory was also applied to the proposed model in order to show how the elements of the system contribute to the operation of the whole system. In the next chapter, this research project will be concluded.

CHAPTER 6: CONCLUSION

6.1 Background

The purpose of this research project was to investigate what security controls could be implemented to protect critical information infrastructure from cyberattacks. Chapter 1 identified the research problem, which was further broken down into three sub-problems. Chapter 2 (sub-problem 1) examined vulnerabilities in critical information infrastructure, while chapter 3 (sub-problem 2) discussed cyberattacks created by cyberthreats. Chapter 4 (sub-problem 3) focussed on a variety of security controls needed to protect critical information infrastructure. In chapter 5, a model to address insecure critical information infrastructure was formulated with the aim of answering the main research question. This chapter will conclude by evaluating the three sub-questions and the proposed model in order to show that the main research question has been answered. Lastly, future research related to this research project will be discussed.

6.2 Evaluation of Sub-problems and Proposed Model

Chapter 1 discussed the research problem, which stated that most organisations do not secure their critical information infrastructure effectively and are thus vulnerable to cyberattacks. This research problem was turned into the main research question which was: **What security controls can be implemented to effectively secure critical information infrastructure and prevent cyberattacks?** In order to answer the main research question, it was further broken down into three sub-questions. These three sub-questions and the proposed model will be summarised below.

Sub-question 1: What types of vulnerabilities may critical information infrastructure possess?

Chapter 2 focused on examining different types of vulnerabilities in critical information infrastructure. Before a number of vulnerabilities were identified, the exploitation of vulnerabilities existing in critical information infrastructure was briefly discussed. The Common Criteria Model (Common Criteria, 2005) was then examined in order to understand the security concepts and relationships, as well as vulnerabilities. The first vulnerability which was discussed was software vulnerabilities, which comprised of unpatched systems and lack of input validation. Next, password vulnerabilities, the most common type of vulnerability which is exploited, were discussed. Personnel vulnerabilities due to naive and disgruntled employees were also examined. This was followed by disaster recovery planning vulnerabilities involving

personnel. The final vulnerability examined in this chapter was network protocol vulnerabilities, which are exploited in order to launch DDoS attacks and allow attackers to create malicious websites to steal confidential information.

Sub-question 1 was answered by identifying various vulnerabilities in critical information infrastructure. As a result, organisations can take measures to rectify these vulnerabilities and prevent them from being exploited.

Sub-question 2: What kinds of cyberthreats create cyberattacks?

In chapter 3, a number of cyberthreats that create cyberattacks were discussed in detail. These cyberthreats exploit various vulnerabilities, which were examined in chapter 2. The internet as a medium used for cyberattacks was briefly discussed in order to emphasise how cyberthreats attack critical information infrastructure via the internet. Throughout this chapter, a number of past events involving organisations which were attacked by cyberthreats were also discussed. This was done in order to emphasise that the research problem exists. The first cyberthreat which was examined was malware including its three categories: viruses, worms and Trojan horses. This group of cyberthreats are capable of stealing information, corrupting it, thus making it unavailable to authorized users in the required format. Another cyberthreat which was discussed was Distributed Denial of Service (DDoS) attacks which are launched in order to take down websites. Next, cyberwarfare was examined which also uses Distributed Denial of Service attacks to take down government websites. This shows that there is a link between different types of cyberthreats. Cyberespionage and cybersabotage were also discussed and are related to cyberwarfare as they are used to steal confidential information, destroy it and make this information unavailable to users. Finally social engineering was discussed and its two categories: phishing and baiting. Both these categories of social engineering focus on the human element in order to trick users into giving out their personal information.

Sub-question 2 was answered by identifying different cyberthreats which create cyberattacks, while referring to various past events involving organisations who were victims of cyberattacks. This was done in order to emphasise that the main research problem exists.

Sub-question 3: What security controls are available to protect critical information infrastructure from cyberattacks?

In chapter 4, preventive, detective and corrective controls were examined. In addition, risk strategies needed to implement these controls were discussed. The General Systems Theory was discussed while applying it to these three controls, which together form a system of controls.

Next defence-in-depth was discussed in order to show how these three controls are used in layers to protect critical information infrastructure. The defend strategy was briefly discussed and is used to implement preventive controls. These preventive controls prevent cyberthreats from entering a system. Policies are an essential preventive control, as all other security controls must comply with policies set by an organisation. Other preventive controls which were discussed included: firewalls, intrusion prevention systems, penetration testing, antivirus software, patches and anti-social engineering techniques. Next, detective controls used to detect cyberthreats which have evaded preventive controls were discussed. This included selecting a mitigation strategy in order to implement these detective controls. Detective controls which were examined included antivirus software, intrusion detection systems and honeypots. Finally, corrective controls used to remove cyberthreats from a system and recover from damages were discussed. This included antivirus software, disaster recovery plans, patches and zombie zappers, which are implemented by using the mitigation control strategy.

Sub-question 3 was answered by identifying and discussing various security controls needed to prevent, detect and correct cyberattacks, thus protecting critical information infrastructure. This included identifying risk strategies needed to implement these three controls. The proposed model will be evaluated next.

Evaluation of Proposed Model

In chapter 4, a model to address insecure critical information infrastructure was formulated. It was based on chapters 2, 3 and 4 and included the research problem. The proposed model was aligned to the research problem, as it depicted how cyberthreats exploit vulnerabilities in order to infiltrate or disrupt insecure critical information infrastructure. To solve this problem, a risk strategy was first selected in order to implement specific security controls. This ensured that the confidentiality, integrity and availability of information were preserved. The proposed model incorporated the General Systems Theory, which indicated that all sub-systems and their elements are needed (as input) to contribute to the operation of the whole system, which consequently resulted in reduced risks to information (output).

After answering sub-questions 1, 2 and 3, as well as formulating and discussing the proposed model, the research question has been answered.

6.3 Future Research

Future research should investigate a specific cyberthreat in more detail which targets a certain part of critical information infrastructure. Thus, the focus could be placed on DDoS attacks which target telecommunications networks. This is an important research area, as users are becoming more dependent on the internet for information. Specific security controls which counter DDoS attacks should be examined in detail, to ensure that information is continuously available to users. The militaryôs use of defence-in-depth could be investigated in more detail, which could be used to protect critical information infrastructure from DDoS attacks.

6.4 Summary

The aim of this research project was to identify security controls that could be used to protect critical information infrastructure from cyberattacks. An extensive literature review was done by using critical thought when reading various sources of information from different authors. Next, a proposed model to address insecure critical information infrastructure was formulated in order to solve the research problem. This was done by selecting risks strategies which were used to implement specific security controls. This ensured that the confidentiality, integrity and availability of information was preserved and as a result, risks to information were reduced.

Definition of Terms

- **Common Criteria Model:** a model which shows security concepts and relationships (Common Criteria, 2005).
- **Critical Information Infrastructure:** information systems that store, process and deliver information (Department of Homeland Security, 2011).
- **Critical Infrastructure:** assets which are critical for the operation of a nationôs economy (Department of Communications, 2014).
- **Cyberattack:** a criminal act which is committed by using computers in order to damage or disrupt systems and networks (GTAG1, 2005).
- **Cyberthreat:** a malicious attempt to damage or disrupt a system or network (Cyberthreat, n.d.).
- **General Systems Theory:** states that a system, within an environment, is made up of elements which are interdependent and contribute to the operation of the whole system (Lin et al., 2012).
- **Security controls:** countermeasures which are used to avoid, counteract or reduce security risks (Northcutt, n.d.).
- **Vulnerability:** a flaw in a system or protection mechanism that exposes a system to cyberattacks (Whitman et al., 2012).

References

Arbor Networks. (2012). *Why IPS Devices and Firewalls Fail to Stop DDoS Threats How to Protect Your Data Center's Availability* [White paper]. Retrieved from http://www.security-finder.ch/fileadmin/dateien/pdf/experten/Why_Firewalls_and_Intrusion_Prevention_Systems_Fall_Short_on_DDoS_Protection-3.pdf

Bandwidth. (n.d.). In *Merriam-Webster's online dictionary*. Retrieved July 30, 2014, from http://www.merriam-webster.com/dictionary/bandwidth

Bell, L. (2014, July 2). Top ranking malware affecting businesses is a Windows XP worm. *The Inquirer*. Retrieved from http://www.theinquirer.net/inquirer/news/2353280/top-ranking-malware-affecting-businesses-is-a-windows-xp-worm#

Bradbury, D. (2013). Information warfare: a battle waged in public. *Computer Fraud & Security*, 2013(6), 15-18.

Brewster, T. (2014, June 4). Life sentences for serious cyberattacks are proposed in Queen's speech. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2014/jun/04/life-sentence-cybercrime-queens-speech/print

Choo, K. R. (2011). The cyber threat landscape: Challenges and future. *Computers and Security*, 30(8), 719-731.

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

Common Criteria. (2005). *ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model.*

Cyberthreat (n.d.). In *Oxford Dictionaries*. Retrieved July 25, 2014, from http://www.oxforddictionaries.com/definition/english/cyberthreat

Davies, C. (2014, March 14). Target reportedly ignored credit card hack warnings. *Slash Gear*. Retrieved from http://www.slashgear.com/target-reportedly-ignored-credit-card-hack-warnings-14320673/

Denning, J. P., & Denning, E. D. (2010, September 9). Discussing cyber attack. *Communications of the A*CM, 53(9), 29-31.

Department of Communications. (2014). The National Integrated ICT Policy Green Paper. South Africa. *Government Gazette*. (No. 37261).

Department of Homeland Security. (2011). *Blueprint for a Secure Cyber Future*. United States of America: Department of Homeland Security.

Everett, C. (2009). The lucrative world of cyber-espionage. *Computer Fraud & Security*, 2009(7), 5-7.

Finkle, J. (2014, July 31). U.S. warns retailers about malicious software stealing credit cards. *The Globe and Mail*. Retrieved from http://www.theglobeandmail.com/technology/us-warns-retailers-about-malicious-software-stealing-credit-cards/article19871690/

Finnan, D. (2014, July 25). Kenyan Army ógood Targetôfor Cyber Attacks and Weôll Carry Out More, Says Anonymous. *allAfrica*. Retrieved from http://allafrica.com/stories/201407251454.html

Fisher, T. (n.d.). *Patch*. Retrieved June 18, 2014, from http://pcsupport.about.com/od/termsp/g/patch-fix.htm

Flowerday, S., & von Solms, R. (2007). What constitutes information integrity? South *African Journal of Information Management*, 9(4), 1-19.

Goel, S. (2011, August 8). Cyberwarfare: connecting the dots in cyber intelligence. *Communications of the ACM*, 54(8), 132-140.

Guerrini, F. (2014, June 17). Brazil's World Cup Of Cyber Attacks: From Street Fighting To Online Protest. *Forbes*. Retrieved from http://www.forbes.com/sites/federicoguerrini/2014/06/17/brazils-world-cup-of-cyber-attacks-from-street-fighting-to-online-protest/

Hassell, J. (2005). *How to limit false positives in IPSes*. Retrieved June 29, 2014, from http://searchsecurity.techtarget.com/tip/How-to-limit-false-positives-in-IPSes

Hunter, S. O., & Irwin, B. (2011). Tartarus: A honeypot based malware tracking and mitigation framework. *Proceedings of the Information Security for South Africa Conference*. Johannesburg: IEEE.

ISO/IEC. (2005). *ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management*. Geneva: ISO/IEC.

James, D. (2012). *Is Your Company Safe From The Disgruntled Employee?* Retrieved June 20, 2014, from http://www.ascentor.co.uk/2012/07/company-safe-disgruntled-employee/

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993.

Jayawal, V., Yurcik, W., & Doss, D. (2002). Internet Hack Back: Counter Attacks as Self-Defence or Vigilantism? *Proceedings of the IEEE International Symposium on Technology and Society (ISTAS)* (pp. 380-386). Raleigh: IEEE.

Jenik, A. (2009). Cyberwar in Estonia and the Middle East. *Network Security*, 2009(4), 4-6.

Jones, A. (2005). Information Warfare ï what has been happening? *Computer Fraud & Security*, 2005(11), 4-7.

Jordan, S. (2012). *Defense in Depth: Employing a Layered Approach for Protecting Federal Government Information Systems* [White paper]. Retrieved June 17, 2014, from SANS Institute: http://www.sans.org/reading-room/whitepapers/bestprac/defense-depth-employing-layered-approach-protecting-federal-government-information-system-34047

Kaspersky. (2013). *Corporate threats*. Retrieved September 18, 2014, from http://report.kaspersky.com/#corporate-threats

Kirk, J. (2014, July 30). No patch yet for zero day in Symantec Endpoint Protection software driver. *PC World*. Retrieved from http://www.pcworld.com/article/2460040/no-patch-yet-for-zero-day-in-symantec-endpoint-protection-software-driver.html

Knake, R. K. (2011). *Internet Governance in an Age of Cyber Insecurity*. New York: Council on Foreign Relations.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2013). Social engineering attacks on the knowledge worker. *Proceedings of the 6th International Conference on Security of Information and Networks* (pp. 28-35). New York: ACM.

Lin, Y., Duan, X., Zhao, C., & Da Xu, L. (2012). *Systems Science: Methodological Approaches.* CRC Press.

Meunier, P. (2008). Classes of vulnerabilities and attacks. *Wiley Handbook of Science and Technology for Homeland Security.*

Mitchell, B. (n.d.). *Protocol (network).* Retrieved July 1, 2014, from http://compnetworking.about.com/od/networkprotocols/g/protocols.htm

Morrow, R. K. (n.d.). Telecommunications network. *Encyclopaedia Britannica*. Retrieved from http://www.britannica.com/EBchecked/topic/585829/telecommunications-network/76420/Spread-spectrum-multiple-access

Musthaler, L. (2013). *Best practices to mitigate DDoS attacks*. Retrieved July 4, 2014, from http://www.networkworld.com/article/2162683/infrastructure-management/best-practices-to-mitigate-ddos-attacks.html

Newman, R. C. (2006). Cybercrime, identity theft, and fraud: practicing safe internet - network security threats and vulnerabilities. *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 68-78). New York: ACM.

Northcutt, S. (n.d.). *Security Controls*. Retrieved June 26, 2014, from http://www.sans.edu/research/security-laboratory/article/security-controls

Northcutt, S., Shenk, J., Shackleford, D., Rosenberg, T., Siles, R. & Mancini, S. (2006). *Penetration Testing: Assessing Your Overall Security Before Attackers Do* [White paper]. Retrieved June 20, 2014, from SANS Institute: http://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635

Olivier, M. S. (2009). *Information Technology Research: A practical guide for Computer Science and Informatics Third Edition*. Pretoria: Van Schaik Publishers.

Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR)*, 39 (1), 1-42.

Praprotnik, G., Ivanuġa, T., & Podbregar, I. (2013). eWar - Reality of Future Wars. *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (pp. 1068-1072). New York: ACM.

Rapoza, K. (2013, June 22). U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press. *Forbes*. Retrieved from http://www.forbes.com/sites/kenrapoza/2013/06/22/u-s-hacked-china-universities-mobile-phones-snowden-tells-china-press/

Richards, D. A., Oliphant, A. S., & Le Grand, H. C. (2005). *Global Technology Audit Guide (GTAG) 1: Information Technology Risks and Controls*. Altamonte Springs: The Institute of Internal Auditors.

Rouse, M. (2010a). *Cyberwarfare*. Retrieved June 24, 2014, from http://searchsecurity.techtarget.com/definition/cyberwarfare

Rouse, M. (2010b). *Cybercrim*e. Retrieved April 20, 2014, from http://searchsecurity.techtarget.com/definition/cybercrime

Schuchart, W. (2013). *5 Reasons Your Employees Don't Care About Business Continuity*. Retrieved June 19, 2014, from http://www.informationweek.com/5-reasons-your-employees-dont-care-about-business-continuity/d/d-id/1110724

Solomon, H. (2014, June 23). Justice staff fall for phishing ploy. *IT World Canada.* Retrieved from http://www.itworldcanada.com/post/justice-staff-fall-for-phishing-ploy

Sood, A. K. (2009). From vulnerability to patch: the window of exposure. *Network Security*, 2009(2), 14-16.

Strickland, J. (2008). *Is cyberwar coming?* Retrieved March 31, 2014, from Howstuffworks: http://computer.howstuffworks.com/cyberwar.htm

Twitchell, D. P. (2006). Social Engineering in Information Assurance Curricula. *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 191-193). New York: ACM.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security Fourth Edition*. Boston: Cengage Learning.

Won, K., Ok-Ran, J., Chulyun, K., & Jungmin, S. (2010). *On Botnets. Proceedings of the 12th International Conference on Information Integration and Webbased Applications & Services* (pp. 5-10). New York: ACM.

Won, K., Ok-Ran, J., Chulyun, K., & Jungmin, S. (2011). The dark side of the Internet: Attacks ,costs and responses. *Information Systems*, 36 (2011), 675-705.

Appendix A: Research Article

Controls for Protecting Critical Information Infrastructure from Cyberattacks

Tamir Tsegaye
201113929
Department of Information Systems
University of Fort Hare
tamir.tsegaye@gmail.com

Stephen Flowerday
Supervisor
Department of Information Systems
University of Fort Hare
sflowerday@ufh.ac.za

ABSTRACT

Critical information infrastructure has enabled organisations, including governments and businesses, to store large amounts of information on their systems and deliver this information via networks such as the internet. Users who are also connected to the internet are able to access various internet services such as e-commerce which are provided by critical information infrastructure. However, some organisations have not effectively secured their critical information infrastructure and hackers, disgruntled employees and other entities have taken advantage of this by using the internet as a medium to launch cyberattacks on their critical information infrastructure. They do this by using cyberthreats to exploit vulnerabilities in critical information infrastructure which organisations fail to secure. Once a vulnerability has been exploited, cyberthreats will consequently be able to steal or damage confidential information stored on systems, or take down organisationsô websites and prevent authorized users from accessing information. Thus, the confidentiality, integrity and availability of information will not be maintained. Despite this, risk strategies can be used to implement a number of security controls: preventive, detective and corrective controls, which together form a system of controls. This will ensure that the confidentiality, integrity and availability of information is preserved, thus reducing any risks to information. This system of controls is based on the General Systems Theory, which states that the elements of a system are interdependent and contribute to the operation of the whole system. Finally, a model is proposed to address insecure critical information infrastructure.

Keywords: Cyberattacks, Critical Information Infrastructure, Vulnerabilities, Cyberthreats, Security Controls

1. INTRODUCTION

Cyberattacks have been targeting critical information infrastructure which is the information systems that store, process and deliver information (Department of Homeland Security, 2011). In 2013, a survey was conducted by Kaspersky Lab and B2B International, indicating that 91% of organisations who took part in the survey had been hit by a cyberattack at least once in a 12-month period, while 9% became victims of cyberattacks (Kaspersky, 2013). Thus, cyberattacks have escalated recently as Choo (2011) emphasises that cyberattacks are increasing in variety and volume. It is important that emphasis is placed on cyberattacks, as anyone possessing a virus infected computer and an internet connection can launch a cyberattack.

These cyberattacks occur in cyberspace i.e the internet, where organisations face many cyberthreats (Department of Communications, 2014). Thus, the internet is used as a medium for cyberattacks. Jordan (2012) explains why the internet was invented: to be used to do research between academic institutions, as well as the US Department of Defence (DOD). Thus it was not designed for security, as its purpose back then was to exchange information between small networks. Due to the emergence of various cyberthreats, security is now essential as information online needs to be protected. Hence, Information Security has been added and aims to protect the confidentiality, integrity and availability of information stored on systems, which form the CIA Triad (ISO/IEC 27002, 2005). Confidential information must be protected from being exposed to unauthorized individuals (Whitman & Herbert, 2012). The integrity of information indicates that information must be complete and not corrupted. Finally, information must only be available to authorized individuals without any interference. These three principles must be maintained in order to effectively secure critical information infrastructure and will be referred to throughout this article.

2. BACKGROUND

In this article, cyberattacks launched on organisationsô vulnerable critical information infrastructure will be examined. Focus will be placed only on the information side of critical infrastructure, thus excluding critical infrastructure such as power stations and water supply systems. Section 3 will discuss a number of vulnerabilities possessed by critical information infrastructure. Next, section 4 will examine various cyberthreats which create cyberattacks that launch attacks on critical information infrastructure. This will be followed by section 5 which will discuss security controls that are needed to protect critical information infrastructure. Finally, in section 6 a proposed model will be examined in order to address insecure critical information infrastructure. This proposed model implements the General Systems Theory which

states that a system, within an environment, is made up of elements that are interdependent and contribute to the operation of the whole system (Lin, Duan, Zhao, Da & Xu, 2012).

3. VULNERABILITIES POSSESSED BY CRITICAL INFORMATION INFRASTRUCTURE

A vulnerability is a flaw in a system or protection mechanism that exposes a system to cyberattacks (Whitman et al., 2012). Attackers can use cyberthreats to exploit vulnerabilities in order to steal confidential information, damage information or take down websites, thus making information unavailable to authorized users.

Figure 1 shows the Common Criteria Model which depicts security concepts and relationships. These security concepts and relationships will be examined before discussing the various types of vulnerabilities which are possessed by critical information infrastructure. By applying this model to critical information infrastructure, owners refer to organisations who value their assets. These assets represent information which is stored on systems and delivered via networks such as the internet.

On the other hand, threat agents may wish to abuse or damage these assets by stealing confidential information, sabotaging or modifying information and preventing access to information. Thus, the CIA principles will not be maintained. Examples of threat agents include hackers, disgruntled employees and other entities. These threat agents give rise to threats which target assets. Examples of threats include malware, cybersabotage and Distributed Denial of Service (DDoS) attacks. These cyberthreats are discussed in section 4. Threat agents are often successful in damaging or abusing assets as they exploit vulnerabilities which are present in critical information infrastructure.

However, owners may be aware of vulnerabilities in critical information infrastructure and thus impose countermeasures (i.e. security controls: discussed in section 5) to reduce them. As a result, risks to assets will be reduced. In contrast, countermeasures such as antivirus software may possess vulnerabilities, which will prevent them from identifying and rectifying the latest software vulnerabilities. Software vulnerabilities will be discussed in the next section.

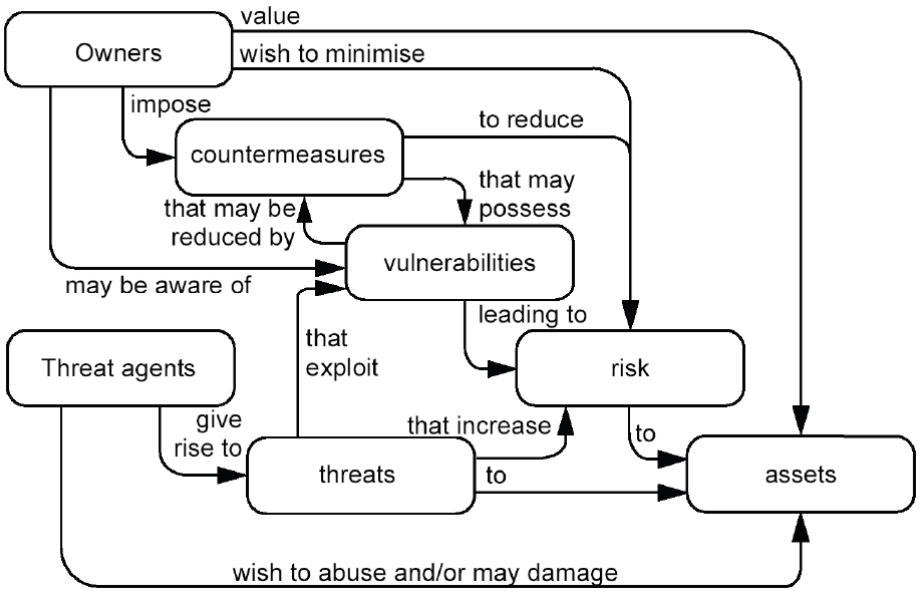

Figure 1: Common Criteria Model (Common Criteria, 2005)

3.1 Software Vulnerabilities

A software vulnerability is a flaw in the design of a computer program (Jang-Jaccard & Nepal, 2014). It is these flaws which malware exploits in order to gain unauthorized access to a system. Once access has been gained, the system is at the disposal of the attacker who launches the cyberattack. Although computer programs such as database software can be beneficial for organisations working with large amounts of information, a vulnerability in this software can potentially cause the information stored in the database to be accessible to the attacker.

3.1.1 Unpatched systems

Unpatched systems create an opportunity for malware to exploit, which leaves a system open to attack (Peng, Leckie & Ramamohanarao, 2007). Despite this, many software programs notify users when new patches are available, which can be installed automatically and secure any vulnerabilities. The lack of input validation in software is another vulnerability which will be discussed next.

3.1.2 Lack of Input Validation

Lack of input validation in web applications is another software vulnerability that can lead to SQL injections, which allow hackers to retrieve confidential information such as credit information from a database (Jang-Jaccard et al., 2014). Thus, input which is submitted on a website should be verified to make sure that it meets certain rules. Although validation is implemented, password vulnerabilities will still be exploited. Password vulnerabilities will be examined next.

3.2 Password Vulnerabilities

Password vulnerabilities consist of weak passwords and are the most common type of vulnerability which is exploited by attackers (Won, Ok-Ran, Chulyun & Jungmin, 2011). Weak passwords such as an employeeôs name and date of birth will easily get exploited by an attacker. Due to this, an attacker can guess a userôs password and gain access to their personal information. By exploiting password vulnerabilities, an attacker does not need to bother finding other vulnerabilities to exploit. Personnel vulnerabilities consisting of disgruntled and naive employees will be discussed next.

3.3 Personnel Vulnerabilities

Personnel vulnerabilities comprise of employees who have the potential to damage their organisationôs information (Colwill, 2009). Disgruntled employees have an advantage over external attackers, as most employees have access to confidential information and know where critical systems are located in their organisation. In contrast, external attackers would need to probe a system and look for vulnerabilities to exploit before they can infiltrate a system.

However, personnel vulnerabilities do not only include disgruntled employees. According to Choo (2011) external attackers are able to take advantage of naive employees in order to steal their confidential information. For example, an attacker could send an email to an employee requesting their password in order to keep their email account active. As a result, employees may carelessly give away their passwords. These methods are used in social engineering which is discussed in section 4.6. Disaster recovery planning vulnerabilities which involves personnel will be examined next.

3.4 Disaster Recovery Planning Vulnerabilities

A disaster recovery plan is a document which specifies the activities that need to be followed to recover from a disaster (Whitman et al., 2012). However, this plan may contain several vulnerabilities. Due to these vulnerabilities, an organisation may not be able to recover information which has been lost due to a cyberattack. A disaster recovery plan which is not tested regularly in a specific scenario will not be reliable in the event of a disaster (GTAG1, 2005). An example of a scenario could include a DDoS attack which has taken down a website. The disaster recovery plan is an important security control and will be discussed in section 5.3.2. Next, vulnerabilities in network protocols will be discussed.

3.5 Network Protocol Vulnerabilities

Some network protocols are vulnerable to cyberattacks and are exploited in order to disrupt or compromise websites (Peng et al., 2007). One vulnerable protocol is Hypertext Transfer Protocol (HTTP). HTTP is exploited by DDoS attacks in order to take down websites, thus preventing access to information. Domain Name System (DNS) is another vulnerable protocol (Jang-Jaccard et al., 2014). The HTTP and DNS protocols are both targeted by DDoS attacks. Attackers exploit this protocol which allows them to create malicious websites used to steal confidential information from victims. Thus it is important that organisations take measures to prevent these protocols from being exploited.

It is evident that a number of vulnerabilities in critical information infrastructure are creating an opportunity for attackers to exploit. As a result, critical information infrastructure will remain insecure. In section 5 a system of controls will be used to address the vulnerabilities which were discussed in this section. Cyberattacks created by cyberthreats will be examined next.

4. CYBERATTACKS CREATED BY CYBERTHREATS

Many organisations have suffered from cyberattacks that have been created by a variety of cyberthreats. These cyberthreats use the internet as a medium to create cyberattacks. They exploit a large number of vulnerabilities in order to infiltrate or take down systems and networks. A number of vulnerabilities which cyberthreats exploit were discussed in the previous section. A common cyberthreat known as malware will be discussed below.

4.1 Malware

Malware is software which is used to compromise a system (Won et al., 2011). It includes three categories: viruses, worms and Trojan horses. Malware can be disguised as legitimate software, which organisations may install erroneously, infecting their systems in the process. This could happen due to the use of ineffective security controls which leave a system open to attack. Jang-Jaccard et al. (2014) describe the growing threat of malware by stating that due to the increase in internet speeds and its affordability, more and more users are connecting to it, causing the threat of malware to increase with it. It is evident that there is a trade-off between the number of internet users and malware. Malware would be stopped if the internet was shutdown, but that is impossible as the internet has been providing beneficial internet services to users. The threat of malware has also been on the increase due to an increase in easy-to-use malware toolkits which are available to anyone for a certain price. For example, the Zeus bot malware creator kit was sold to novice users with detailed instructions on how to use it (Choo, 2011). Thus, this has created opportunities for amateur hackers to steal confidential information such as credit card

information and passwords. Malware infected computers are used to launch DDoS attacks and will be discussed next.

4.2 Distributed Denial of Service

Distributed Denial of Service is an attack which uses a group of infected computers to take down a website, by flooding it with unnecessary traffic (Praprotnik, Ivanuġa & Podbregar, 2013). Many countries such as Estonia have been hit by DDoS attacks, which have negatively affected their economy. For instance, in 2007 Estoniaôs government and ecommerce websites were brought down by DDoS attacks (Jenik, 2009). As a result, users were not able to access their online banking accounts and thus could not make any transactions. DDoS attacks are used extensively in cyberwarfare which will be discussed next.

4.3 Cyberwarfare

Cyberwarfare comprises of several other cyberthreats such as DDoS, cyberespionage and cybersabotage. It includes hackers and governments who attack systems or networks belonging to other governments (Goel, 2011). Anyone with a computer and an internet connection can take part in cyberwarfare intentionally or unintentionally (if their computer is turned into a zombie). Cyberespionage used by various attackers will be examined below.

4.4 Cyberespionage

One area of cyberwarfare is cyberespionage, which is the use of computers to steal confidential information from systems (Praprotnik et al., 2013). For instance, hackers may be employed by their government to steal classified information from other governments. Everett (2009) elaborates on this by stating that a developing nation may use cyberespionage in order to catch up with first world nations. Alternatively, an organisation may plan to steal trade secrets from another organisation and use it to improve their competitive advantage in their industry. The last part of cyberwarfare, cybersabotage, will be discussed next.

4.5 Cybersabotage

Cybersabotage, which is another area of cyberwarfare, includes damaging information and defacing or taking websites (Goel, 2011). Hacktivists may protest against the government by using DDoS attacks to take down or deface their websites. For example, during the Russia-Georgia war in 2008, Russian hacktivists disabled and defaced Georgian government web sites using cyberattacks (Goel, 2011). In contrast, disgruntled employees can sabotage information by installing malware on their organisationôs systems (Won et al., 2011). However, an employee may unintentionally create an opportunity for their organisation to be attacked. This will be discussed next under social engineering.

4.6 Social Engineering

Social engineering is a method used by attackers to deceive employees into giving them their confidential information (Newman, 2006). Even if an organisation secures its systems effectively, employees who are easily tricked may unknowingly let malware enter their system. Malware will enter the system if preventive controls such as antivirus software do not exist. There are various types of methods used in social engineering such as phishing and baiting. Phishing is used a lot in social engineering and will be discussed next.

4.6.1 Phishing

Phishing is a method which is used to obtain confidential information from innocent people, by masquerading as a trustworthy source (Jang-Jaccard et al., 2014). These innocent people may receive an email from an attacker requesting their passwords for a certain reason. The victim then clicks a link in the email which directs them to a malicious website belonging to the attacker. Any information entered onto this website is sent to the attacker. For instance, in 2010 cybercriminals sent phishing emails (with the Zeus malware attached to it) that targeted employees who were in charge of IT operations in the USA (Choo, 2011). Once the phishing email was opened, the Zeus malware was installed on the victimôs system and consequently stole their confidential information. Thus it is important that employees are able to differentiate between an authentic website and a phishing website. Another method used in social engineering known as baiting is examined below.

4.6.2 Baiting

Baiting involves an attacker who leaves a malware infected storage media such as a flash drive in an area, where it can easily be found by the targeted victim (Krombholz, Hobel, Huber & Weippl, 2013). This flash drive could have a label such as ñconfidentialò to tempt the victim to take a look at its content on their computer. For example, the flash drive could be dropped on an organisationôs premises by an attacker targeting a specific employee. The employee may then insert the flash drive into their computer. As a result, the malware will get installed on the computer, allowing the attacker to remotely control it. Hence, the organisationôs computer may end up being used to launch a DDoS attack on another organisation.

CYBERTHREAT		VULNERABILITIES
4.1	**Malware**	• **Software vulnerabilities**: exploit unpatched systems in order to infiltrate a system (Peng et al., 2007). • **Personnel vulnerabilities**: naive users may be tempted to download legitimate software disguised as a Trojan horse, which consequently infect their system (Colwill, 2009).
4.2	**Distributed Denial of Service (DDoS)**	• **Network protocol vulnerabilities**: HTTP protocol exploited in order to take down websites (Peng et al., 2007).
4.3	**Cyberwarfare**	• **Software vulnerabilities**: malware used to steal and damage information (Won et al., 2011). • **Personnel vulnerabilities**: disgruntled employees may sabotage their organisationôs systems (Newman, 2006). • **Network protocol vulnerabilities**: DDoS attacks take down websites by exploiting HTTP protocol (Peng et al., 2007).
4.6	**Social Engineering**	• **Personnel vulnerabilities**: users tricked into giving their personal information (Newman, 2006).

Table 1: Vulnerabilities Exploited by Cyberthreats

Based on section 4, cyberthreats exploit vulnerabilities in critical information infrastructure in order to steal, corrupt or make information unavailable. Hence, the three CIA principles will not been maintained. In the next section security controls will be identified in order to counter these cyberthreats which were discussed in this section.

5. SECURITY CONTROLS USED TO PROTECT CRITICAL INFORMATION INFRASTRUCTURE

Security controls comprise of three categories: preventive, detective and corrective controls. Preventive controls prevent security incidents from happening, while detective controls detect any security incidents that have avoided preventive controls. Lastly, corrective controls correct incidents which have been detected. Both technical and non-technical controls will be discussed in this section. An organisation should have more preventive controls compared to detective and corrective controls, as preventing a cyberthreat from attacking a system or network is the best defence.

Figure 2 shows some control classifications. General controls comprise of access controls and disaster recovery plans. Governance controls consist of policies while management controls include separation of duties. On the other hand, technical controls include antivirus software and firewalls. Application controls are not included in this article. All of these controls mentioned

above can be put into the three categories of preventive, detective and corrective controls. Preventive controls, which are the first line of defence, will be discussed next.

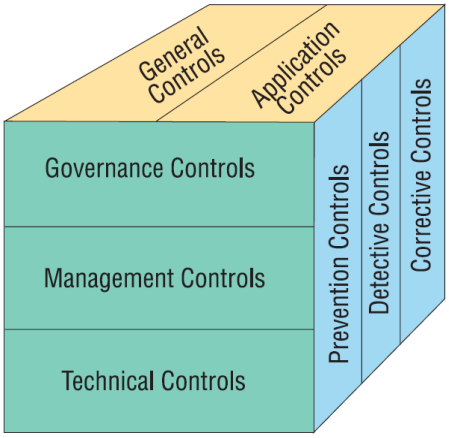

Figure 2: Some Control Classifications (GTAG1, 2005)

5.1 Preventive Controls

Before preventive controls are implemented, a risk strategy such as the defend strategy needs to be selected. The defend strategy attempts to prevent the exploitation of vulnerabilities (Whitman et al., 2012). This is achieved by implementing preventive controls, such as policies, which will be examined next.

5.1.1 Policies

Policies are rules which are set by the board of directors and executive management of an organisation (GTAG1, 2005). Policies are implemented to help increase the level of security in an organisation. Some policies which could be implemented include allowing people to only access specific information based on their role. In addition, security education, training and awareness programs should be included to ensure that employees do not fall for phishing scams (Northcutt, n.d.). All security controls should comply with policies, such as firewalls which are discussed next.

5.1.2 Firewalls

A firewall is a security control which is used to manage incoming and outgoing network traffic and determines if the traffic should be allowed through based on certain rules (Jang-Jaccard et al., 2014). For example, traffic coming from outside an organisationôs network is analysed by the firewall to check if it meets certain rules specified by the firewall. If it does not meet any of these rules, the firewall will prevent the traffic from entering the network. A firewall is useful as

it allows organisations to define their own firewall rules which should comply with policies. An intrusion prevention system is another preventive control which is discussed next.

5.1.3 Intrusion Prevention Systems

An intrusion prevention system is used to prevent cyberthreats from entering a system or network, as well as detect cyberthreats which have been found on a system or network (Whitman et al., 2012). Hence, an intrusion prevention system acts as both a preventive and detective control. Won et al. (2011) mention two methods used by intrusion prevention systems; the first method used is known as signature-based detection (also used by antivirus software), where signature definitions are checked to see if incoming traffic matches any known signatures. On the other hand, anomaly-based detection is used to monitor traffic as it occurs and compares it to ónormalô traffic based on statistics which are stored over time. Anomaly-based detection is useful as an alternative method, in the event that signature-based detection misses detecting any malicious traffic. Penetration testing, another preventive control used to test security controls, will be discussed next.

5.1.4 Penetration Testing

Penetration testing is a set of security tests that simulate attacks made by an external attacker (Whitman et al., 2012). These security tests are done in order to identify vulnerabilities in networks and systems. These vulnerabilities can then be rectified once they are found. Hence, penetration testing is a preventive control as once vulnerabilities are identified and secured; cyberthreats will be prevented from entering systems or networks. Antivirus software, which is another preventive control, will be discussed next.

5.1.5 Antivirus Software

Antivirus software is not only a preventive control but also a detective and corrective control (Northcutt, n.d.). It acts as a preventive control by preventing malware from attacking a system, which may steal confidential information or corrupt it. It is important that antivirus software is updated regularly to protect systems from the latest malware. Patches, which are used to update antivirus software and other programs, will be examined below.

5.1.6 Patches

A patch is software which is used to update or fix a programôs problems (Fisher, n.d.). Besides fixing these problems, its major use is to address software vulnerabilities. Once a patch has been applied to an unpatched system, vulnerabilities will be secured. Thus, cyberthreats will be prevented from entering a system. Won et al. (2010) mention an example where vendors provide updates to prevent zombie computers from exploiting software vulnerabilities. Most software

programs allow patches to be updated automatically, but it is up to the user to select this setting. It is important that updates are installed automatically, as employees may forget to do so manually. Anti-social engineering techniques used to counter phishing (which was discussed in section 4.6.1), will be discussed next.

5.1.7 Anti-social Engineering Techniques

There are different techniques which can help prevent employees from becoming victims of social engineering scams such as phishing. Twitchell (2006) mentions an example such as providing security training to employees in order to raise awareness on phishing methods used by attackers. Policies can also be implemented such as ensuring that the latest internet browser updates are installed regularly. This will help internet browsers to identify any malicious signs on a website and warn employees beforehand. Won et al. (2011) elaborate by stating that internet browsers display pop-up windows, warning users of any suspicious signs which have been detected on a website. Despite this, employees may overlook these warnings. As a result, they may enter their credentials on a malicious website although they were warned in advance. The second layer of security: detective controls will be discussed in detail below.

5.2 Detective Controls

In the event that a cyberthreat has been able to bypass preventive controls, detective controls would ensure that the cyberthreat is identified. A mitigation strategy, which is another type of risk strategy, would need to be selected before implementing detective controls (Whitman et al., 2012). This strategy aims to reduce the impact caused by the exploitation of a vulnerability, which has allowed a cyberthreat to infiltrate a network or system. A mitigation strategy is important as it ensures that attacks are detected early. A number of detective controls will be examined below.

5.2.1 Antivirus Software

Antivirus software functions as a detective control by alerting a user when malware has been found on a system (Northcutt, n.d.). An example of this would be a message which appears, warning a user that a threat has been detected e.g. after a flash drive has been plugged into a system. An intrusion detection system is another detective control which is discussed next.

5.2.2 Intrusion Detection Systems

An intrusion detection system is used to detect suspicious activity which has been found on a system or network. If any suspicious activity has been found, an administrator will be alerted by the intrusion detection system (Won et al., 2012). As a result, they can take action before a cyberthreat attacks the system or network. Honeypots, which are also able to detect suspicious activity, will be examined next.

5.2.3 Honeypots

A honeypot is a decoy system which is used to gather information, by recording the activities performed by the attacker who infiltrated the honeypot (Jang-Jaccard et al., 2014). This information can be used to learn about an attackerôs motives, including the methods of attacks used by the attacker. Thus, organisations will be able to protect themselves from future attacks. Corrective controls which are the third and final layer will be examined below.

5.3 Corrective Controls

Corrective controls are used once a cyberthreat has managed to bypass preventative controls and evade detective controls. A mitigation strategy would need to be used to implement corrective controls, which will respond to an attack as quickly as possible (Whitman et al., 2012). A number of corrective controls will be discussed next.

5.3.1 Antivirus Software

Antivirus software acts as a corrective control by removing any malware which has been found on a system (Won et al., 2012). This malware could have damaged or stolen confidential information from a system. Although antivirus software can remove malware which has infected a system, it is not able to recover information which may have been corrupted or destroyed. A disaster recovery plan can address this issue and is discussed next.

5.3.2 Disaster Recovery Plan

A disaster recovery plan is a document which specifies the activities which are followed, in order to recover from a disaster (Whitman et al., 2012). Backing up information is an important part of this plan and should be done on a regular basis, as organisations store large amounts of information on their systems. Thus, a disaster recovery plan acts as a corrective control since information which has been corrupted by malware can be recovered from backups. Next, patches as a corrective control will be discussed.

5.3.3 Patches

Patches do not only function as a preventive control but are also used as a corrective control, as they fix flaws which have been found in software programs (Fisher, n.d.). The vulnerability which a cyberthreat may have exploited is patched so that the same vulnerability cannot be exploited in the future. However, new vulnerabilities may be discovered, thus the latest patches should be regularly applied when available. The final corrective control which will be discussed next is Zombie Zapper.

5.3.4 Zombie Zapper

Zombie Zapper is a free tool which is used as a corrective control. It can be used to command a zombie computer to stop flooding a network with traffic (Jenik, 2009). This will help organisations save money instead of looking for some other commercial tool to stop DDoS attacks.

Hence, various security controls are available to counteract cyberattacks in the form of preventive, detective and corrective controls. It is important that organisations do not only use one of these controls as the only layer of security, but should use other controls as well. In the next section a model is proposed to address insecure critical information infrastructure.

PREVENTIVE	DETECTIVE	CORRECTIVE
5.1.1 Policies	5.2.1 Antivirus Software	5.3.1 Antivirus Software
5.1.2 Firewalls	5.2.2 Intrusion Detection Systems	5.3.2 Disaster Recovery Plan
5.1.3 Intrusion Prevention Systems	5.2.3 Honeypots	5.3.3 Patches
5.1.4 Penetration Testing		5.4.4 Zombie Zapper
5.1.5 Antivirus Software		
5.1.6 Patches		
5.1.7 Anti-social Engineering Techniques		

Table 2: Categories of Security Controls

6. PROPOSED MODEL

6.1 Model to Address Insecure Critical Information Infrastructure

The proposed model depicted in Figure 3 aims to address insecure critical information infrastructure. Cyberthreats exploit vulnerabilities in critical information infrastructure in order to infiltrate or disrupt it. Cyberthreats do this with the aim of stealing, corrupting or making information unavailable to users. To counter these cyberthreats, risk strategies are needed to implement specific security controls. The risk strategies depicted in this model are the defend strategy and mitigation strategy. The defend strategy is used to prevent the exploitation of vulnerabilities in critical information infrastructure, while the mitigation strategy is used to reduce the impact caused by the exploitation of vulnerabilities. Once risk strategies have been selected and security controls have been implemented, they will ensure that the confidentiality, integrity and availability of information are ensured. As a result, risks to information will be reduced

The proposed model is a differentiated model, which uses certain elements from the Common Criteria Model (Common Criteria, 2005) and the CIA Triad Model (ISO/IEC 27002, 2005). These two models are both general models (Olivier, 2009). The original CIA Triad Model does not illustrate any elements that show how the confidentiality, integrity and availability of information are preserved. On the other hand, the proposed model illustrates how risk strategies and security controls can be used to ensure that the CIA principles are preserved.

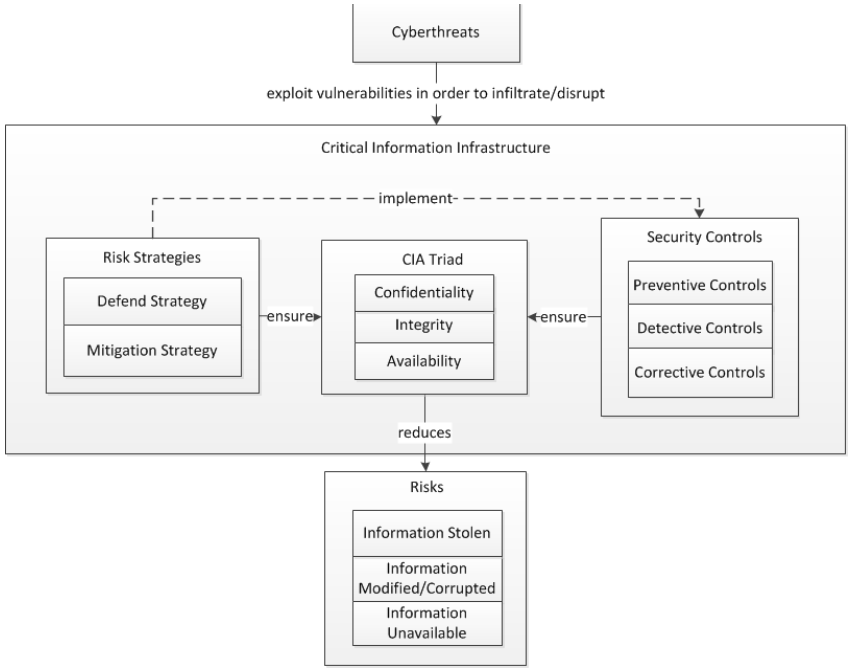

Figure 3: Model to Address Insecure Critical Information Infrastructure

6.2 Application of General Systems Theory to Proposed Model

The General Systems Theory states that a system, within an environment, is made up of elements which are interdependent and contribute to the operation of the whole system (Lin et al., 2012). This system has inputs which are processed into outputs.

By applying the General Systems Theory to the proposed model, critical information infrastructure is the overall system and is made up of three elements (i.e. sub-systems) which contribute to the functioning of the overall system. These three sub-systems are: risk strategies, the CIA Triad and security controls (system of controls). Each sub-system is further broken down into its elements. Thus, the General Systems Theory is hierarchical as it has different levels.

The first sub-system, risk strategies, is made up of the defend strategy and mitigation strategy elements. Both of these strategies are needed to implement all three controls. The second sub-system is the CIA Triad and is made up of three elements: confidentiality, integrity and availability. The CIA Triad can only be made a ówholeô with all three elements. The third sub-system is security controls. This sub-system is made up of preventive, detective and corrective controls. If preventive, detective or corrective controls are missing, critical information infrastructure will be vulnerable to cyberattacks. For instance, if a cyberthreat bypasses preventive controls and detective controls are missing, it will not be detected. Thus, all three controls are needed to form a system of controls.

Hence, if any elements of the three sub-systems are excluded, then the output (reduced risks) will not be achieved.

These three sub-systems (and their elements) are used as input, while the process consists of selecting a specific risk strategy to implement security controls.

7. CONCLUSION

Although critical information infrastructure has allowed organisations to store and deliver information via the internet, vulnerabilities exist, which makes critical information infrastructure vulnerable to cyberattacks. Cyberthreats create these cyberattacks and are consequently able to steal and corrupt information or make it unavailable to authorized users, by denying access to internet services such as online banking. Despite this, security controls are available to counter these cyberthreats. Before security controls are used, a risk strategy needs to be implemented. Thus, the confidentiality, integrity and availability of information will be preserved and risks to information will be reduced.

8. REFERENCES

Choo, K. R. (2011). The cyber threat landscape: Challenges and future. *Computers and Security*, 30(8), 719-731.

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

Department of Communications. (2014). The National Integrated ICT Policy Green Paper. South Africa. *Government Gazette*. (No. 37261).

Department of Homeland Security. (2011). *Blueprint for a Secure Cyber Future*. United States of America: Department of Homeland Security.

Everett, C. (2009). The lucrative world of cyber-espionage. *Computer Fraud & Security*, 2009(7), 5-7.

Fisher, T. (n.d.). *Patch*. Retrieved June 18, 2014, from http://pcsupport.about.com/od/termsp/g/patch-fix.htm

Goel, S. (2011, August 8). Cyberwarfare: connecting the dots in cyber intelligence. *Communications of the ACM*, 54(8), 132-140.

ISO/IEC. (2005). *ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management*. Geneva: ISO/IEC.

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5), 973-993.

Jenik, A. (2009). Cyberwar in Estonia and the Middle East. *Network Security*, 2009(4), 4-6.

Jordan, S. (2012). *Defense in Depth: Employing a Layered Approach for Protecting Federal Government Information Systems* [White paper]. Retrieved June 17, 2014, from SANS Institute: http://www.sans.org/reading-room/whitepapers/bestprac/defense-depth-employing-layered-approach-protecting-federal-government-information-system-34047

Kaspersky. (2013). *Corporate threats*. Retrieved September 18, 2014, from http://report.kaspersky.com/#corporate-threats

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2013). Social engineering attacks on the knowledge worker. *Proceedings of the 6th International Conference on Security of Information and Networks* (pp. 28-35). New York: ACM.

Lin, Y., Duan, X., Zhao, C., & Da Xu, L. (2012). *Systems Science: Methodological Approaches.* CRC Press.

Meunier, P. (2008). Classes of vulnerabilities and attacks. *Wiley Handbook of Science and Technology for Homeland Security.*

Northcutt, S. (n.d.). *Security Controls*. Retrieved June 26, 2014, from http://www.sans.edu/research/security-laboratory/article/security-controls

Olivier, M. S. (2009). *Information Technology Research: A practical guide for Computer Science and Informatics Third Edition*. Pretoria: Van Schaik Publishers.

Peng, T., Leckie, C., & Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys (CSUR), 39 (1), 1-42.

Praprotnik, G., Ivanuġa, T., & Podbregar, I. (2013). eWar - Reality of Future Wars. *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining* (pp. 1068-1072). New York: ACM.

Richards, D. A., Oliphant, A. S., & Le Grand, H. C. (2005). Global Technology Audit Guide (GTAG) 1: Information Technology Risks and Controls. Altamonte Springs: The Institute of Internal Auditors.

Twitchell, D. P. (2006). Social Engineering in Information Assurance Curricula. *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 191-193). New York: ACM.

Whitman, M. E., & Mattord, H. J. (2012). *Principles of Information Security Fourth Edition*. Boston: Cengage Learning.

Won, K., Ok-Ran, J., Chulyun, K., & Jungmin, S. (2011). The dark side of the Internet: Attacks, costs and responses. Information Systems, 36 (2011), 675-705.