Defending Critical Information Infrastructure from Cyberattacks through the Use of Security Controls in Layers

Tamir Tsegaye, Stephen Flowerday
Department of Information Systems
University of Fort Hare
East London, South Africa

Abstract

Critical information infrastructure has enabled organisations to store large amounts of information on their systems and deliver it via networks such as the internet, providing users with internet services. However, some organisations have not effectively secured their critical information infrastructure and hackers, disgruntled employees and other entities have taken advantage of this by launching cyberattacks on their critical information infrastructure. They do this by using cyberthreats to exploit vulnerabilities in critical information infrastructure which organisations fail to secure. As a result, cyberthreats are able to steal or damage confidential information stored on systems or take down websites, preventing access to information. 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. These security controls are used in layers to increase the level of security. This will ensure that the confidentiality, integrity and availability of information is preserved, thus reducing 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.

1. Introduction

Cyberattacks have been targeting critical information infrastructure, which is the information systems that store, process and deliver information [1]. These cyberattacks have escalated lately, increasing in variety and volume [2]. Hackers, disgruntled employees and other entities are capable of launching cyberattacks. It is important that emphasis is placed on cyberattacks, as anyone possessing a virus infected computer and an internet connection can launch a cyberattack.

Many organisations have been hit by cyberattacks as a result of not securing their systems and networks. A survey was conducted by Kaspersky Lab and B2B International in 2013. It indicated 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 [3]. In addition, in 2013 Spamhaus was attacked by one of the biggest Distributed Denial of Service (DDoS) attacks to date, with the attack reaching a throughput of 300gbps [3].

The internet was originally invented for the purpose of conducting research between academic institutions, as well as the US Department of Defence (DOD) [4]. 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 which aims to protect the confidentiality, integrity and availability of information stored on systems [5]. Confidentiality, integrity and availability are the three principles of information and form the CIA Triad [6]. Confidential information must be protected from being exposed to unauthorized individuals. The integrity of information indicates that information must be complete and not corrupted. Finally, information must be available to authorized individuals without any interference. These three principles of information must be preserved in order to effectively secure critical information infrastructure. The impact that cyberthreats have on the CIA principles will be referred to throughout this paper.

In this paper, cyberattacks launched on organisations' 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 2 will discuss a number of vulnerabilities possessed by critical information infrastructure. Next, section 3 will examine various cyberthreats which create cyberattacks that target critical information infrastructure. This will be followed by section 4 which will discuss security controls which are needed to protect critical information infrastructure. Section 4 will also discuss the military strategy of defence-in-depth which emphasises the use of security controls in layers. Finally, in section 5 a proposed model will be examined in order to address insecure critical information infrastructure.

2. Vulnerabilities in Critical Information Infrastructure

A vulnerability is a flaw in a system or protection mechanism that exposes a system to cyberattacks [5]. 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.

Fig. 1 shows the Common Criteria Model which depicts security concepts and relationships [7]. 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 this paper, 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.

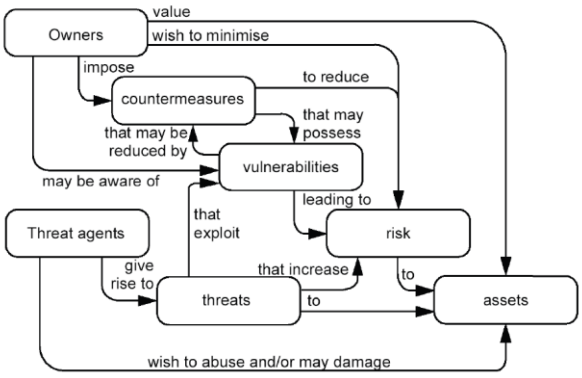

Figure 1. Common Criteria Model [7]

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 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 attacks (discussed in section 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: discussed in section 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.

2.1. Software Vulnerabilities

A software vulnerability is a flaw in the design of a computer program [8]. 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. Two categories of software vulnerabilities: unpatched systems and lack of input validation will be examined next.

2.1.1. Unpatched Systems. Unpatched systems create an opportunity for malware to exploit, which leaves a system open to attack [9]. Despite this, many software programs notify users when new patches are available, which can be installed automatically and secure any vulnerabilities.

Organisations such as Microsoft release a number of patches every year [10]. 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. Lack of input validation in software is another vulnerability which is discussed below.

2.1.2. Lack of Input Validation. Input validation is a process which ensures that input data follows certain rules [8]. 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, such as cybercriminals, can enter SQL commands into fields in order to retrieve confidential information from the databases of 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 discussed next.

2.2. Password vulnerabilities

Password vulnerabilities consist of weak passwords and are one of the most common vulnerabilities exploited by attackers [11]. Weak passwords such as an employee's name and date of birth can get exploited by an attacker. Due to this, an

attacker can easily guess an employee's password and gain access to their personal information. By exploiting a password vulnerability, an attacker does not need to use another method such as phishing (discussed in section 3.4.1) to steal a user's passwords. Vulnerabilities in passwords arise due to systems which allow users to use passwords that are short or passwords which only contain the letters of the alphabet [11]. In addition, the policies of many organisations do not require users to change their passwords after a period of time. Hence, this has led to an increase in the amount of vulnerable passwords which are still used and exploited today.

Weak passwords can be exploited through the use of various methods. For instance, a dictionary attack can be used to easily guess the most commonly used passwords which users may be using [12]. Attackers control zombies (infected with malware) which use this method to crack vulnerable passwords. Thus, it is crucial that users use strong passwords to avoid their passwords from being compromised. Personnel vulnerabilities consisting of disgruntled and naive employees will be discussed next.

2.3. Personnel Vulnerabilities

Personnel vulnerabilities comprise of employees who have the potential to damage their organisation's information [13]. 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. External attackers are able to take advantage of naive employees in order to steal their confidential information [2]. 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 3.4. Disaster recovery planning vulnerabilities which involves personnel will be examined next.

2.4. 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 [5]. 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 that is not tested regularly in a specific scenario will not be reliable in the event of a disaster [14]. 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 4.4.2. Next, vulnerabilities in network protocols will be discussed.

2.5. Network Protocol Vulnerabilities

Some network protocols are vulnerable to cyberattacks and are exploited in order to disrupt or compromise websites [9]. 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 [8]. 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 4, security controls will be used to address the vulnerabilities which were discussed in this section. Cyberattacks created by cyberthreats are covered in the next section.

3. 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 examined next.

3.1. Malware

Malware is software which is used to compromise a system [11]. 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. 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 [8]. 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 rise 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 [2]. Thus, this has created opportunities for amateur hackers to steal confidential information such as credit card information and passwords.

Malware is also used to infect computers which take part in DDoS attacks [15]. This has occurred in the past with the Conficker worm which created a botnet of around six million zombies, used to launch DDoS attacks on organisations [16]. Thus, it is evident that worms are also able to create opportunities for other cyberthreats to attack such as Distributed Denial of Service which is discussed below.

3.2. Distributed Denial of Service

Distributed Denial of Service is an attack which uses a group of infected computers (also known as a botnet) to take down a website by flooding it with unnecessary traffic [15]. Many countries have been hit by DDoS attacks which have negatively affected their economy. For example, in 2007 Estonia's government and ecommerce websites were brought down by DDoS attacks [17]. As a result, users were not able to access their online banking accounts and thus could not make any transactions.

A DDoS attack takes place as follows: all of the infected computers simultaneously send a request to a targeted website via a command from an attacker [11]. The target is then forced to reply to the requests made by zombies and due to the large amount of traffic generated, may not be able to cope and thus shutdown. The attacker is hard to identify since their IP address is spoofed as the infected computers' 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.

DDoS attacks are not only launched by experienced attackers. Anyone can rent or buy a botnet from a cybercriminal for a certain price [18]. 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 not only launch DDoS attacks, but to also send phishing emails. This is another reason why there has been an increase in the number of cyberattacks as botnets are easily available. DDoS attacks are used extensively in cyberwarfare which will be discussed next.

3.3. 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 [16]. 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 will be examined below.

3.3.1. Cyberespionage. One area of cyberwarfare is cyberespionage which is the use of computers to steal confidential information from systems [15]. For instance, hackers may be employed by their government to steal classified information from other governments. In addition, a developing nation may use cyberespionage in order to catch up with first world nations [18]. Alternatively, an organisation may plan to steal trade secrets from another organisation and use it to improve their competitive advantage in their industry.

An example of the theft of intellectual property occurred in 2009 where Chinese hackers launched a cyberattack on various organisations, including Google and Yahoo [16]. These hackers were able to exploit a software vulnerability in Internet Explorer, allowing them to install malware on the organisations' computers. As a result, the Chinese hackers were able to steal intellectual property which was found on the compromised computers belonging to various organisations. An attacker can also choose to damage information via cybersabotage which is discussed next.

3.3.2. Cybersabotage. Cybersabotage, which is another area of cyberwarfare, includes damaging information and defacing or taking down websites [16]. Hacktivists may protest against the government by using DDoS attacks to take down or deface their websites. For instance, during the Russia-Georgia war in 2008, Russian hacktivists disabled and defaced Georgian government web sites using cyberattacks [16].

Modifying information illegally to reflect inaccurate information is also part of cybersabotage [10]. For example, an attacker may decide to alter the prices of goods sold on an ecommerce website, causing users to pay the wrong amount of money for a product.

On the other hand, disgruntled employees can sabotage information by installing malware on their organisation's systems [10]. However, an employee may unintentionally create an opportunity for their organisation to be attacked. This will be discussed next under social engineering.

3.4. Social Engineering

Social engineering is a method used by attackers to deceive employees into giving them their confidential information [10]. Even if an organisation secures its systems effectively, employees who are easily tricked may unknowingly let malware enter these systems. Malware will enter their systems if preventive controls such as antivirus software do not exist. There are various methods used in social engineering such as phishing and baiting. Phishing is used a lot in social engineering and will be discussed next.

3.4.1. Phishing. Phishing is a method which is used to obtain confidential information from innocent people by masquerading as a trustworthy source [8]. 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.

Phishing is not only used to lure victims to malicious websites, but is also used to infect them with malware [8]. 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 [2]. Once the phishing email was opened, the Zeus malware was installed on the victim's system and consequently stole their confidential information [2].

In addition, hackers use botnets to send excessive amounts of phishing emails [12]. 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 attacker using their own computer to send phishing emails. It is important that organisations are aware of both phishing and DDoS attacks, as both of these cyberthreats involve the use of botnets to launch cyberattacks. Another method used in social engineering known as baiting is examined below.

3.4.2. 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 [19]. This flash drive could have a label such as "confidential" to tempt the victim to take a look at its content on their computer. For example, the flash drive could be dropped on an organisation's 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. Thus, the organisation's computer may end up being used to launch a DDoS attack on another organisation.

Based on section 3, cyberthreats exploit vulnerabilities in critical information infrastructure in order to steal, corrupt or make information unavailable. Hence, the three CIA principles will not be preserved. Table 1 shows the vulnerabilities exploited by cyberthreats which were covered earlier on. In the next section, security controls will be identified in order to preserve the CIA principles.

Table 1. Vulnerabilities Exploited by Cyberthreats

CYBERTHREAT		VULNERABILITIES
3.1.	**Malware**	• **Software vulnerabilities**: exploit unpatched systems in order to infiltrate a system [9]. • **Personnel vulnerabilities**: naive users may be tempted to download legitimate software disguised as a Trojan horse, which consequently infects their system [13].
3.2.	**Distributed Denial of Service (DDoS)**	• **Network protocol vulnerabilities**: HTTP protocol exploited in order to take down websites [9].
3.3.	**Cyberwarfare**	• **Software vulnerabilities**: malware used to steal and damage information [11]. • **Personnel vulnerabilities**: disgruntled employees may sabotage information stored on their organisation's systems [10]. • **Network protocol vulnerabilities**: DDoS attacks take down websites by exploiting HTTP protocol [9].
3.4.	**Social Engineering**	• **Personnel vulnerabilities**: users tricked into giving their personal information [10].

4. Security Controls Used to Protect Critical Information Infrastructure

With the variety of cyberthreats 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 [20]. These security controls are put into three categories: preventive, detective and corrective controls [14]. Preventive controls prevent security incidents from happening, while detective controls detect any security incidents that have avoided preventive controls. 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.

These controls can also be put into other categories as depicted in Fig. 2 which shows some control classifications [14]. Both general and governance controls consist of policies (discussed in section 4.2.1), while the category of management controls includes separation of duties. On the other hand, technical controls include firewalls (discussed in section 4.2.2). Application controls ensure that input data is validated, thus preventing the exploitation of the lack of input validation (which was discussed earlier in section 2.1.2.). Security controls should be used in layers to increase the level of security and will be covered next under defence-in-depth.

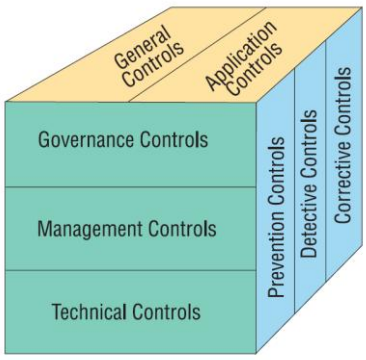

Figure 2. Some Control Classifications [14]

4.1. Defence-in-depth

Defence-in-depth is a military strategy which is also used in information security. It specifies the use of multiple security controls in layers to successfully protect information in the event that one or more security controls fail [21]. Implementing multiple security controls in layers will ensure that an attack which is in progress can be identified quickly and countered before information is compromised. However, if a vulnerability exists in a security control which has been implemented by an organisation, then the control would be ineffective and the control would not be able to prevent, detect or correct the cyberthreat. Thus, by using the strategy of defence-depth, more than one control should be implemented so that if a cyberthreat manages to bypass an ineffective control, another control should be present to counter the attack.

Fig. 3 depicts the sphere of security which shows that information is at the center of this sphere and is at risk from cyberattacks [5]. In order to gain access to this information, the attacker launching a cyberattack from the internet would need to first penetrate an organisation's network and then infiltrate their systems. However, employees do not need to penetrate the network and may have access directly to critical systems containing confidential information.

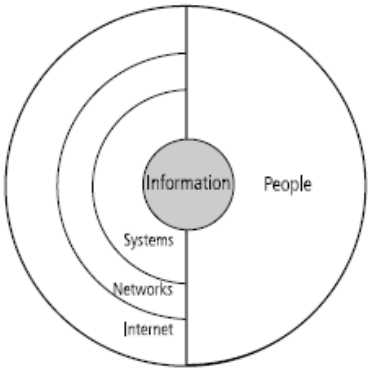

Figure 3. Sphere of Security [5]

The defence-in-depth strategy can be applied to this model whereby multiple security controls can be applied between each layer of the sphere. For example, security controls implemented between the internet and networks layer would include firewalls and intrusion prevention systems. The right-half of the sphere shows that people (i.e. employees in an organisation) have access to networks, systems and information. In this instance, non-technical controls such as policies and security education, training and awareness programs would be needed. This will help to reduce the risk of information being compromised due to naive or disgruntled employees.

Some security controls can be used to protect more than one layer [21]. For example, a hardware firewall can be used to protect the networks layer, while a software firewall can also be used to protect the systems layer. Thus, if malicious traffic manages to bypass a hardware firewall, the software firewall would be able to drop the traffic, if it has the relevant rule configured. Preventive controls, which are the first line of defence, will be discussed next.

4.2. 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 [5]. This is achieved by implementing preventive controls such as policies.

4.2.1. Policies. Policies are rules which are set by the board of directors and executive management of an organisation [14]. 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 [20]. All security controls should comply with policies such as firewalls [14].

4.2.2. Firewalls. A firewall is a security control which is used to manage incoming and outgoing network traffic and determines if traffic should be allowed through based on certain rules [8]. For example, traffic coming from outside an organisation's 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. Another preventive control which also manages traffic is an intrusion prevention system and will be discussed next.

4.2.3. Intrusion Prevention Systems. An intrusion prevention system is a security control which is able to prevent cyberthreats from entering a system or network [5]. Once malicious traffic has been detected, an intrusion prevention system can drop the traffic, thus preventing unauthorized access to a network. Preventive methods used by an intrusion prevention system include filtering or rate-limiting [11]. Using an intrusion prevention system in combination with a firewall can decrease the chance of a cyberthreat penetrating a network, thus emphasising the concept of defence-in-depth. The detection methods used by an intrusion prevention system to detect malicious traffic will be discussed in section 4.3.1. Antivirus software is another preventive control which is examined next.

4.2.4. Antivirus Software. Antivirus software is not only a preventive control, but also a detective and corrective control [20]. 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. Next, penetration testing which acts as a preventive control is discussed.

4.2.5. Penetration Testing. Penetration testing is a set of security tests that simulate attacks made by an external attacker [5]. These security tests are done in order to identify vulnerabilities in networks and systems. These vulnerabilities can then be secured once they are found. Hence, penetration testing is a preventive control as once vulnerabilities have been identified and secured, cyberthreats will be prevented from entering systems or networks. Patches can also prevent cyberthreats from entering a system and are discussed below.

4.2.6. Patches. Patches can be applied to software in order to address software vulnerabilities, such as unpatched systems, which were discussed in section 2.1.1 [4]. Thus, cyberthreats will be prevented from entering a system which has the latest patches installed. Most software programs allow patches to be updated automatically, but it is up to the user to select this setting [12]. It is important that updates are installed automatically as employees may forget to do so manually. Detective controls, which are the second layer of security, will be examined next.

4.3. 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 [5]. 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.

4.3.1. Intrusion Prevention Systems. An intrusion prevention system does not only act as a preventive control, but can be configured to also act as a detective control [20]. Two methods are used to detect cyberthreats present on a system or network: signature-based detection and anomaly-based detection [11]. Signature-based detection consists of signature definitions which are checked to see if incoming traffic matches any known signatures. If a match has been found, the intrusion prevention system will raise an alarm to alert the administrator. The second method is anomaly-based detection which an intrusion prevention system uses to monitor traffic as it occurs and compares it to 'normal' traffic based on statistics which are stored over time. If

abnormal traffic is detected, the intrusion prevention system will alert the administrator about any suspicious activity which has been found on 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. Antivirus software which uses similar detection methods is covered below.

4.3.2. Antivirus Software. Antivirus software functions as a detective control by alerting a user when malware has been found on a system [11]. An example of this would be a message which appears, warning a user that malware has been detected e.g. after a flash drive has been plugged into a system.

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 [11]. 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. On the downside, some attackers are capable of altering virus signatures [15]. 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 a zombie. The methods of detection used by antivirus software are also used by intrusion detection systems, which are discussed next.

4.3.3. 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 [11]. As a result, action can be taken before a cyberthreat attacks a system or network.

Intrusion detection systems use the same methods of detection as intrusion prevention systems which were explained earlier on [8]. An intrusion detection system is useful as it is able to detect malicious traffic which may have bypassed a firewall.

However, an intrusion detection system is not effective if it is the only detective control which is used. For instance, in 2009 a group of hackers infiltrated the network of various organisations in the USA [16]. 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 organisations' systems. Hence, it is crucial that organisations do not only rely on an intrusion detection system to protect their confidential information, but should use it in combination with another detective control. Honeypots, which are also able to detect suspicious activity, will be examined next.

4.3.4. 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 [8]. This information can be used to learn about an attacker's motives, including the methods of attack used by the attacker. Thus, organisations will be able to protect themselves from future attacks.

Honeypots can also be used to analyze botnets in order to find ways to counter them [8]. Fortunately, there will be no confidential information stored on the honeypot for the attacker to steal or destroy. However, due to the popularity of honeypots today, attackers have found ways to prevent them from falling into these traps. Tools such as "Send-Safe Honeypot Hunter" are used by attackers to detect honeypots [12]. Thus if attackers use this tool, they will avoid honeypots. As a result, the logs used to store the attackers' activities will be empty. Corrective controls which are the third and final layer of security will be discussed next.

4.4. Corrective Controls

Corrective controls are used once a cyberthreat has managed to bypass preventive 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 [5]. A number of corrective controls will be discussed below.

4.4.1. Antivirus Software. Antivirus software acts as a corrective control by removing any malware which has been found on a system [11]. 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.

4.4.2. Disaster Recovery Plan. A disaster recovery plan is a document which specifies the activities which are followed in order to recover from a disaster [5]. 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. The final corrective control which will be discussed next is Zombie Zapper.

4.4.3. Zombie Zapper. Zombie Zapper is a free tool which is used to command a zombie to stop flooding

a network with traffic [17]. This tool will help organisations save money instead of looking for some other commercial tool to help counter zombies.

Hence, various security controls are available to counteract cyberthreats in the form of preventive, detective and corrective controls which are depicted in Table 2. 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.

Table 2. Categories of Security Controls

PREVENTIVE	DETECTIVE	CORRECTIVE
Policies [14], [20]	Intrusion Prevention Systems [11], [20]	Antivirus Software [11]
Firewalls [8]	Antivirus Software [11], [15]	Disaster Recovery Plan [5]
Intrusion Prevention Systems [5], [11]	Intrusion Detection Systems [8], [11], [16]	Zombie Zapper [17]
Antivirus Software [20]	Honeypots [8], [12]	
Penetration Testing [5]		
Patches [4], [12]		

5. Proposed Model

The proposed model depicted in Fig. 4 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 preserved. As a result, risks to information will be reduced.

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 [22]. 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. 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 'whole' 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 to information) will not be achieved.

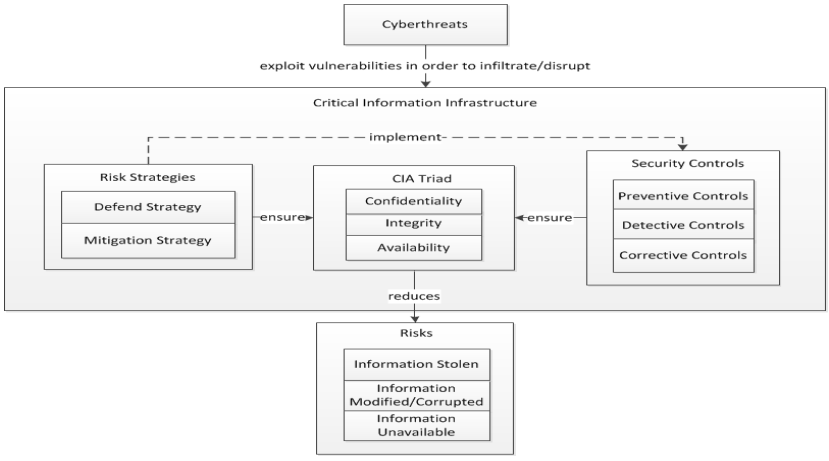

Figure 4. Model to Address Insecure Critical Information Infrastructure

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.

The proposed model is a differentiated model which uses certain elements from the Common Criteria Model and the CIA Triad Model [6] [7]. These two models are both general models [23]. 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.

6. 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 information. Despite this, security controls are available to counter these cyberthreats. Before security controls are used, a risk strategy needs to be selected. Thus, the confidentiality, integrity and availability of information will be preserved and risks to information will be reduced.

7. References

[1] Department of Homeland Security, "Blueprint for a Secure Cyber Future," 2011. http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf (Access Date: 12 September, 2014).

[2] K. R. Choo, "The cyber threat landscape: Challenges and future research directions," *Computers and Security*, vol. 30, no. 1, pp. 719–731, Nov. 2011.

[3] Kaspersky, "Kaspersky Security Bulletin 2013. Malware Evolution," 2013. https://kasperskycontenthub.com/report/files/ksb13_EN_lite-1.pdf (Access Date: 18 September, 2014).

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

[5] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 4 ed. Boston: Course Technology Press, 2012.

[6] International Organization for Standardization and the International Electrotechnical Commission, "ISO/IEC 27002: Information technology – Security techniques – Code of practice for information security management," 2005.

[7] Common Criteria, "ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model," 2005. https://www.commoncriteriaportal.org/files/ccfiles/ccpart1v2.3.pdf (Access Date: 5 September, 2014).

[8] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973-993, Aug. 2014.

[9] T. Peng, C. Leckie and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Computing Surveys (CSUR)*, vol. 39, no. 1, pp. 1-42, 2007.

[10] R. C. Newman, "Cybercrime, identity theft, and fraud: practicing safe internet – network security threats and vulnerabilities," in *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*, New York: ACM, 2006, pp. 68-78.

[11] K. Won, J. Ok-Ran, K. Chulyun, and S. Jungmin, "The dark side of the Internet: Attacks ,costs and responses," *Information Systems*, vol. 36, pp. 675-705, May. 2011.

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

[13] C. Colwill, "Human factors in information security: The insider threat – Who can you trust these days," *Information Security Technical Report*, vol. 14, no. 4, pp. 186-196, Nov. 2009.

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

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

[16] S. Goel, "Cyberwarfare: connecting the dots in cyber intelligence," *Communications of the ACM*, vol. 54, no. 8, pp. 132-140, Aug. 2011.

[17] A. Jenik, "Cyberwar in Estonia and the Middle East," *Network Security*, pp. 4-6, Apr. 2009.

[18] C. Everett, "The lucrative world of cyber-espionage," *Computer Fraud & Security*, pp. 5-7, Jul. 2009.

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

[20] S. Northcutt, "Security Controls," n.d. http://www.sans.edu/research/security-laboratory/article/security-controls (Accessed: 26 June 2014).

[21] J. Andress, *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*, Elsevier, 2011.

[22] Y. Lin, X. Duan, C. Zhao, and L. D. Xu, *Systems Science: Methodological Approaches.* Boca Raton: CRC Press, 2012.

[23] M. S. Olivier, Information Technology Research: A practical guide for Computer Science and Informatics, 3 ed., Pretoria: Van Schaik Publishers, 2009.

