



THE JOURNAL OF  
**DIGITAL FORENSICS,  
SECURITY AND LAW**

**Journal of Digital Forensics,  
Security and Law**

---

Volume 4 | Number 4

Article 3


---

2009

## **Prevention is Better than Prosecution: Deepening the Defence against Cyber Crime**

Jacqueline Fick  
*PricewaterhouseCoopers*

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

---

### **Recommended Citation**

Fick, Jacqueline (2009) "Prevention is Better than Prosecution: Deepening the Defence against Cyber Crime," *Journal of Digital Forensics, Security and Law*: Vol. 4 : No. 4 , Article 3.

DOI: <https://doi.org/10.15394/jdfsl.2009.1066>

Available at: <https://commons.erau.edu/jdfsl/vol4/iss4/3>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact [commons@erau.edu](mailto:commons@erau.edu).



(c)ADFSL



## **Prevention is Better than Prosecution: Deepening the Defence against Cyber Crime<sup>1</sup>**

**Jacqueline Fick**

PricewaterhouseCoopers  
Johannesburg, South Africa  
jacky.fick@za.pwc.com

### **ABSTRACT**

In the paper the author proposes that effectively and efficiently addressing cyber crime requires a shift in paradigm. For businesses and government departments alike the focus should be on prevention, rather than the prosecution of cyber criminals. The Defence in Depth strategy poses a practical solution for achieving Information Assurance in today's highly networked environments. In a world where "absolute security" is an unachievable goal, the concept of Information Assurance poses significant benefits to securing one of an organization's most valuable assets: Information. It will be argued that the approach of achieving Information Assurance within an organisation, coupled with the implementation of a Defence in Depth strategy can ensure that information is kept secure and readily available and provides a competitive advantage to those willing to invest and maintain such a strategy.

**Keywords:** cyber crime, cyber law, defence in depth, layered defence, information assurance, information security, public private partnerships, risk management

### **1. INTRODUCTION AND APPROACH**

The President in his State of the Nation address on 3 June 2009 specifically referred to an increased effort to combat cyber crime and identity theft.

Cyber criminals in South Africa have increased their attacks in both the private and public sector, with the most prevalent (cyber) offence remaining that of identity theft. However, it must be borne in mind that identity theft is in most cases a means to an end: to assume someone's identity to evade the police, to obtain credit on someone else's credentials where the criminal is not able to do

---

<sup>1</sup> A shorter version of this paper was first presented at the Lex Informatica conference held in Johannesburg, South Africa in July 2009. That paper was selected as a best paper by the conference with an extension of that paper to be considered for publication within the Journal of Digital Forensics, Security and Law. The original paper for that presentation was then first published in the October 2009 issue of De Rebus, the South African Attorneys' Journal. Copyright in the original article vests in the Law Society of South Africa (LSSA) and this extended version of the article is published here with the permission of the LSSA.

that on his/her own, to gain access to bank accounts, to launder money, etc.

But at the heart of cyber crime in South Africa lies the true asset these criminals wish to obtain: information. Information has become the most important asset any business or government department has and it is this information that enables a criminal to assume another identity, to log into another's bank account, to steal confidential information, to deny an organisation access to its critical information systems. Yet we fail to protect it with the same vigour as we protect our money or property.

Secondly, South African law enforcement has been hampered in effectively dealing with this breed of criminals, due to for example resource constraints and a lack of sufficient training. We also have no accurate statistics to determine the true value of these crimes, nor the extent to which they have harmed our country.

Dealing with cyber crime in South Africa calls for a shift in paradigm: new investigative methodologies and techniques, an increase in effective public private partnerships, better sharing of business intelligence and information and most importantly, moving from a re-active to a pro-active approach to dealing with cyber crime.

This paper aims to show that prevention is better than prosecution. Devoting time and resources to implement strategies that make it difficult for criminals to perpetrate their crimes within organisations is more efficient and cost effective than trying to catch them after you had been the victim of a cyber attack. And in the unlikely event that you do fall victim to cyber crime and you have the right strategy and systems in place, you would also have a disaster recovery plan in place that enables the organisation to effectively and efficiently deal with the consequences of an attack, an audit trail that can point your investigation in the right direction and evidentiary material available that could stand the scrutiny of a court.

Catching and eventually prosecuting cyber criminals are difficult and costly, both in terms of money, time and resources. For businesses and government alike the reputational damage attached to a cyber attack can also be costly.

The author is of the opinion that implementing the five core principles of Information Assurance and the Defence in Depth strategy, poses significant benefits to the prevention of cyber crime within South African businesses, as well as in government. It will be submitted that the approach of achieving Information Assurance within the organisation, coupled with the implementation of a Defence in Depth strategy can ensure that information is kept secure and provide a competitive advantage to those willing to invest in such a strategy.

## **2. INFORMATION ASSURANCE**

### **2.1 Definition**

Information Assurance is defined in Wikipedia as the practice of managing information-related risks. More specifically, Information Assurance seeks to protect and defend information and information systems by ensuring confidentiality, integrity, authentication, availability and non-repudiation. These goals are relevant whether the information is in storage, processing, or transit and whether threatened by malice or accident. In other words, Information Assurance is the process of ensuring that the right users have access to the right information at the right time.

According to the US Department of Defence Dictionary of Military and Associated Words, 2003 Information Assurance is defined as information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Assurance is closely related to Information Security and the terms are sometimes used interchangeably. However, its broader connotation also includes reliability and emphasises strategic risk management over tools and tactics. In addition to defending against malicious hackers and code, Information Assurance includes other corporate governance issues such as privacy, compliance, audits, business continuity and disaster recovery. Whilst Information Security draws primarily from computer science, Information Assurance is interdisciplinary and draws from multiple fields, including accounting, fraud examination, forensic science, management science, systems engineering, security engineering and criminology, in addition to computer science.

Information Assurance can be viewed as an umbrella concept bringing together issues of information security and dependability. It must always be borne in mind that “absolute security” is an unachievable goal. What the concept of Information Assurance proposes is defined in its name: it is providing organisations with an acceptable level of assurance that even when there are attempts to interfere with the security, availability and reliability of networks and systems, there will still be an acceptable level of functionality.

### **2.2 Objective of Information Assurance**

The objective of Information Assurance is to minimise the risk that information systems and the information stored, transmitted and processed thereon is vulnerable to threats. This implies that, if an attack does take place, the damage it might cause will be minimised. It also provides for a method to recover from the attack as efficiently and effectively as possible.

Information Assurance requires an organisation to focus on its access controls (both physical and logical access controls), individual accountability to ensure that each user of the system can be identified and to provide for audit trails which can provide historical records when a system is compromised.

### **2.3 Five Pillars of Information Assurance**

Information Security is based on what is known as the CIA triad, namely confidentiality, integrity and availability. Information Assurance has an additional two principles namely authenticity and non-repudiation. Together they form the so-called five pillars of Information Assurance.



Figure 1: The five pillars of Information Assurance

The National Security Agency of the United States of America (NSA) recommends that the application of the five pillars of Information Assurance should be based on the Protect, Detect and React paradigm. This means that in addition to incorporating protection mechanisms, organisations need to expect attacks and include attack detection tools and procedures that allow them to react to and recover from these attacks. It further recommends the implementation of a Defence in Depth strategy to achieve Information Assurance. This strategy will be discussed in full below.

Upon analysis of the Electronic Communications and Transactions Act, No. 25 of 2002 (ECT Act), it becomes clear that the five pillars of Information Assurance is entrenched in our legislation and that in most instances, a breach in any of these areas has been criminalised.

#### *2.3.1 Confidentiality*

Keeping information confidential implies that information must only be accessed, used, copied or disclosed by users who have been duly authorised to do so. This would include for example where you allow someone to only view information and not copy it for them, but the person was not authorised to see the information in the first instance.

In terms of section 85 of the ECT Act “access” includes the actions of a person who, after taking note of any data, becomes aware of the fact that he or she is not

authorised to access that data and still continues to access that data. Section 86 of the ECT Act criminalises the unauthorised access to, interception of or interference with data.

In terms of section 86(2), read with section 89(1) a person who intentionally accesses or intercepts data without the authority or permission to do so is guilty of an offence and is liable to a fine or imprisonment not exceeding twelve months.

### *2.3.2 Integrity*

Data integrity also deals with authorisation and implies that data may not be created, altered or deleted without the proper authorisation. A loss of integrity could occur when a computer is infected with a virus, or where someone gains unauthorised accesses to a server and deletes critical data files. Data integrity is also important in cases where computer evidence is to be used in court.

In terms of section 14(1) of the ECT Act, where the law requires that information is to be presented or retained in its original form that requirement is met by a data message if the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment and that information is capable of being displayed or produced to the person to whom it is to be presented.

In terms of section 14(2) the integrity must be assessed by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display, as well as in light of the purpose for which the information was generated and having regard to any other relevant circumstance.

Section 17 stipulates that where a law requires a person to produce a document or information, that requirement is met if the person produces, by means of a data message, an electronic form of that document or information, and if considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document, as well as that at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference. Section 17(2) furthermore provides that the integrity of the information in a document is maintained if the information has remained complete and unaltered, except for the addition of any endorsement, or any immaterial change, which arises in the normal course of communication, storage or display.

Section 86(2), read with section 89(1) of the ECT Act provides that a person who intentionally and without authority to do so, interferes with data in a way which

causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence and is liable for a fine or imprisonment of up to twelve months.

### *2.3.3 Authenticity*

In simple terms authenticity means that a user that logged on to a computer is in reality the person whose credentials (e.g. user name and password) was used, or that documents on a computer have not been altered or forged.

The most common authentication breach in South Africa is where user id's and passwords are stolen (identity theft) and used to load false transactions on a system. One must always bear in mind that identity theft is not when someone steals your credit card number; it is when someone steals *you* (Campana, 2006).

According to Scott Charney from Microsoft (Tung, 2008) much has been done in terms of defence in depth against malware or against phishing schemes, but more remains to be done. For this to happen, better authentication is required so that users can make better decisions about what is running on their computers. Charney also noted that there has been a major shift by software vendors to tie software more tightly to hardware to solve the problem of authentication. According to him one needs operating systems that are bound to the hardware, so that if it is tampered with there is better chance of knowing about, detecting and remediating the problem.

Chapter VI of the ECT Act provides for the authentication of service providers in South Africa where accreditation is defined as the recognition of an authentication product or service by the Accreditation Authority. Authentication products or services are defined as products or services designed to identify the holder of an electronic signature to other persons.

In terms of section 86(3), read with section 89(1) a person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possesses any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section, is guilty of an offence and liable to a fine or imprisonment not exceeding twelve months.

Section 86(4), read with section 89(2) furthermore provides that a person who utilises any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence and liable to a fine or imprisonment not exceeding five years.

#### *2.3.4 Availability*

Availability does not only mean that the information on a system must be readily available, but also that the systems needed to process the information and the security measures that protect the information are all functioning properly at the time the information is needed. In simple terms the right information must be available to the right person at the right time.

During a denial of service (DoS) attack, information is not readily available because the users cannot access the information on their computers. Section 86(5) of the ECT Act, read with section 89(2) provides that a person who commits any act with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial of service to legitimate users is guilty of an offence and liable to a fine or imprisonment not exceeding five years.

#### *2.3.5 Non-repudiation*

Non-repudiation implies that parties to an electronic transaction are bound in terms of that transaction: the one party cannot deny having received the information, nor can the other party deny sending it.

In terms of section 25 of the ECT Act a data message is that of the originator if it was sent by the originator personally, or by a person who had the authority to send it on behalf of the originator, or if it was sent by an information system programmed by or on behalf of the originator to operate automatically, unless it is proved that the information system did not properly execute such programming.

An acknowledgement of receipt of a data message is not necessary to give legal effect to the message, but in terms of section 26 of the ECT Act acknowledgement of receipt may be given by any communication by the addressee, whether automated or otherwise, or any conduct of the addressee, sufficient to indicate to the originator that the data message has been received.

In terms of section 23 of the ECT Act a data message used in the conclusion or performance of an agreement must be regarded as having been sent by the originator when it enters an information system outside the control of the originator or, if the originator and addressee are in the same information system, when it is capable of being retrieved by the addressee. It is also stated that a data message must be regarded as having been received by the addressee when the complete data message enters an information system designated or used for that purpose by the addressee and is capable of being retrieved and processed by the addressee, and must be regarded as having been sent from the originator's usual place of business or residence and as having been received at the addressee's usual place of business or residence.

In electronic commerce digital signatures are commonly used to establish authenticity and non-repudiation. Section 13 of the ECT Act stipulates that where



the signature of a person is required by law and such law does not specify the type of signature, that requirement in relation to a data message is met only if an advanced electronic signature is used.

### **3. DEFENCE IN DEPTH STRATEGY**

#### **3.1 Introduction**

Due to the rapid development of business, IT trends and technology, it has become increasingly important to maintain proper control of an organisations' information. It is now commonly recognised that information is one of (if not) the most valuable assets an organisation has. This information pertains to various business processes and disciplines within a single organisation: ranging from strategic management information to basic operational process information.

Defence in Depth is a strategy that can be implemented to achieve Information Assurance in today's highly networked environments. According to the NSA it is a "best practices" strategy in that it relies on the intelligent application of techniques and technologies that exist today. The strategy is based on balancing protection capability and cost, performance and operational considerations.

In its report on Defence in Depth, the Trusted Information Sharing Network (TISN) defines Defence in Depth as the systematic security management of people, processes and technologies, in a holistic risk-management approach.

The concept is based on military strategy which implements defences primarily to delay rather than prevent the advance of an attacker. It is assumed that an attack will lose momentum over time, allowing for those being attacked to respond appropriately. This strategy is particularly useful when dealing with Information Assurance as one can never rule out the possibility of an attack, but one can implement a strategy that effectively and efficiently guards against, monitors and reports on such attacks and, in the event that an attack does take place provides for a strategy to address the damage.

According to the TISN (TISN, 2008) the Defence in Depth is far more than an IT concept, as it delivers:

- effective risk-based decisions;
- enhanced operational effectiveness;
- reduced overall cost and risk; and
- improved information security.

Defence in Depth provides an approach to security that is integrated with the organisation's business processes and enterprise-wide risk management capability.

For an organisation to effectively protect its information and information systems against cyber attacks, it is necessary to determine who the enemy is, why they

would want to launch an attack against the organisation and how they would then attack the organisation.

Threats to the confidentiality, integrity and availability of an organisation’s information assets can arise through its employees, business partners, external sources and technological innovation. The potential cyber criminal might be a disgruntled employee that aims to commit corporate espionage or launch a denial of service attack, or it might be a cyber syndicate that wants to steal user id’s and passwords to gain access to your client’s bank accounts. Threats can also relate to intentional and unintentional actions that can potentially harm information assets. Examples of these threats include the following (TISN, 2008):

<b>PEOPLE</b>	<b>TRADING PARTNERS</b>
<ul style="list-style-type: none"> <li>• Disgruntled employees</li> <li>• Financially troubled employees</li> <li>• Corporate espionage</li> <li>• Uneducated/uninformed users</li> </ul>	<ul style="list-style-type: none"> <li>• Business partners with poor data security</li> <li>• Physical access to shared systems</li> <li>• Misunderstanding of allowed access</li> <li>• Competitive environment</li> </ul>
<b>EXTERNAL THREATS</b>	<b>TECHNOLOGICAL INNOVATION</b>
<ul style="list-style-type: none"> <li>• Hackers</li> <li>• Organised crime</li> <li>• Changes in regulatory framework</li> </ul>	<ul style="list-style-type: none"> <li>• Faster networks</li> <li>• More storage in smaller devices</li> <li>• Technological convergence</li> <li>• Increasingly mobile workforce</li> </ul>

### **3.2 Focus Areas of Defence in Depth Strategy**

An important principle of the Defence in Depth strategy is that achieving Information Assurance requires a balanced focus on four primary elements, namely People, Technology and Processes (or Operations) and Governance.

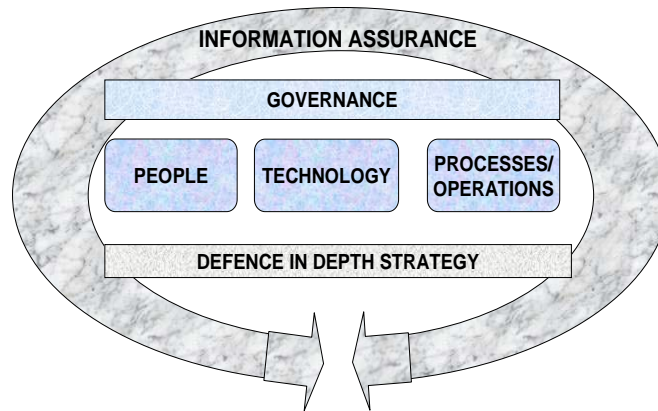


Figure 2: People, Processes, Technology and Governance

Figure 2 outlines the basic principles of a Defence in Depth strategy. The strategy is based on the concepts of technology, people and processes (or Operations), and governed in terms of a management framework.

Furthermore, it is of paramount importance to determine what the organisations' system priorities are. In other words which systems are critical to business operations and are needed to ensure operational effectiveness and a competitive advantage?

### *3.2.1 Technology*

Technology refers to solutions that organisations employ that enable them to achieve and sustain their business objectives. Key focus areas for implementing a Defence in Depth strategy in terms of technology would include the management of network architecture, infrastructure management, application security and communications management.

A wide range of products are available that provide for Information Assurance services and detecting intrusions. It is, however, of paramount importance to ensure that the organisation's procurement policy is aligned to the overall Defence in Depth strategy and that the right technology is procured in accordance with the achievement of overall business objectives. An effective procurement policy and process must have regard to the organisation's security policy, what level of security is needed for a particular application, if the particular product has been validated by a reputable third party, a risk analysis pertaining to the acquisition of the particular technology or product, issues of integration with current systems and processes, etc.

### *3.2.2 People*

Within the context of the Defence in Depth strategy People refers to the security roles and responsibilities for internal and external persons. It is essential to define, maintain and enforce security roles and responsibilities for employees within the organisation, contractors or business partners that the organisation deals with, service providers that are used where functions are outsourced and service providers that supply products or services to the organisation.

Another key focus area would be user awareness and ensuring that all relevant internal and external persons are fully aware of and conversant with their particular role and responsibility and the procedural and governance framework, as well as policies applicable to them.

### *3.2.3 Processes (or Operations)*

Processes (or Operations) refer to the standardised actions which are used to ensure the organisation's position on security is sustained. What this means in terms of the Defence in Depth strategy is that organisations must define, maintain and enforce standardised actions/processes which are used to develop and sustain its position on security on a daily basis.

Key focus areas for the implementation of the strategy would typically include identity and user-access management, incident response management, disaster recovery management and audit management.

The NSA provides the following examples of activities that are traditionally categorised under this heading:

- Maintaining a visible and up to date system security policy.
- Certifying and accrediting changes to the Information Technology baseline. These processes should provide the data to support risk management-based decisions. It should also acknowledge that a "risk accepted by one is a risk shared by many" in an interconnected environment.
- Managing the security posture of the Information Assurance technology (e.g. installing security patches and virus updates and maintaining access control lists).
- Providing key management services and protecting the relevant infrastructure.
- Performing system security assessments, e.g. vulnerability scanners to assess the continued "security readiness" of the organisation.
- Monitoring and reacting to current threats.
- Attack sensing, warning and response.

- Recovery and re-constitution.

#### *3.2.4 Governance*

Within the context of a Defence in Depth strategy, governance refers to the oversight and coordination of technology, people and processes that is provided in terms of a management framework. Key focus areas for the implementation of the Defence in Depth strategy would include risk management, information security and policy and compliance management. Achieving Information Assurance through a Defence in Depth strategy would traditionally begin with commitment from a senior management level (such as from the Chief Information Officer), based on a clear understanding of exactly what the threats are that the organisation is facing. This is then followed up by integrating and aligning the understanding with the organisation's overall strategy, aligning with and incorporating it into with the business objectives and goals, drafting and implementing appropriate policies and deriving suitable procedures from them.

### **3.3 Core Principles of Defence in Depth Strategy**

The TISN (TISN, 2008) defines the core principles of a Defence in Depth strategy as follows:

- Implementing measures according to business risks.
- Using a layered approach which would mean that if a single control fails, it would not result in the whole system being compromised. The concept of a layered approach or layered defence is discussed under paragraph 3.5.
- Implementing controls in such a way that they would increase the effort needed to attack and breach the system.
- Implementing personnel, procedural and technical controls.

In order to successfully implement a Defence in Depth strategy management must include the core principles of this strategy in the organisation's overall strategy, in their annual planning, as well as within their organisational structure.

It is important that the Defence in Depth strategy should not only protect against attacks, but also enable organisations to detect attacks and effectively respond to it. It must also be borne in mind that attacks can take place from multiple locations by people from both inside the organisation or by outsiders. It would therefore be necessary to deploy controls at multiple locations to guard against all classes of attacks.

A further important consideration is that, in case of an attack happening within an organisation, the audit trail must be of such a nature that it would assist the organisation in taking appropriate internal disciplinary steps or that they would be

able to provide sound evidentiary material and assistance to law enforcement agencies where criminal proceedings are to be instituted.

### **3.4 Implementing a Defence in Depth Strategy**

Implementing a Defence in Depth strategy requires a shift in paradigm. Organisations must move away from the notion that IT security and/or Information Assurance are stand-alone issues, to where these concepts become an integral part of business planning, overall strategy, governance and operations.

If one were to explain in practical terms what the importance of achieving Information Assurance is, try to imagine any organisation functioning without IT systems and support and even more pertinently, how any organisation can sustain its proper functioning and competitive advantage without securing, preventing unauthorised access to and insuring availability and functionality of its critical information.

According to the 2009 IDG Research Services Survey some companies are so enthusiastic about the potential of new web and mobile technologies that they deploy them without adequately securing critical processes and data. Implementing a Defence in Depth strategy requires co-ordinating and integrating knowledge of the overall strategy and goals of the organisation or department, the internal environment (including systems, personnel and information assets), and the internal and external threat environment.

The TISN (TISN, 2008) have identified four reasons why it is necessary to implement a Defence in Depth strategy:

- **Expanding organisational boundaries:** Businesses today form close alliances with their business partners, customers and suppliers. This results in hard-to-define external boundaries, for example where business partners form a consortium to deliver a product, it might be that they rely on the same infrastructure, IT systems, personnel, etc. to deliver the specific product. There is a need to determine where the organisations' boundaries lie and what it is that it aims to protect by implementing a Defence in Depth strategy.
- **Mobile workforce:** It has become increasingly important for employees to be able to access their company networks from a remote location. Employees need to access their emails from home or have their mail delivered to a Blackberry device. The close interconnectivity between controls and office networks enable viruses and worms to spread more easily to control systems (Lüders, 2006).
- **Decentralisation of services:** As the use of computers in the workplace increases, so does the provision of services and systems via the intra and extranets. Previously it was only necessary to grant

access to a select few, but these services and systems now have to be provided to a broader set of users.

- **Increasing value of information:** As stated above, businesses have realised what the value of information is to maintaining and sustaining a competitive advantage. Due to the value of information, it has become increasingly important to apply stringent security measures to guard against the loss, destruction, tampering and theft of a businesses' information. It is also important to ensure that the right person has the right access to the right information at the right time.

The steps to implementing a Defence in Depth Strategy can be summarised as follows:

- **Analysis of internal and external environment:** The first step towards implementing a Defence in Depth strategy would be to analyse the internal and external environment in which an organisation operates: what its strengths and weaknesses are, the threats the organisation faces, what systems, assets, technology and processes are being used? It is also necessary to establish what the organisations' overall strategy is, to determine if the Defence in Depth strategy is aligned to business objectives and goals and if there is a clear understanding of what the Defence in Depth strategy means for the organisation, as well as what it would entail to implement it.
- **Determining the risks:** The second step is to determine what risks the organisation faces (in terms of Information Assurance): based on the weaknesses, threats and vulnerabilities that have been identified it is necessary to firstly establish if the organisation is aware of the identified risks and if they understand the implications of such risks. The identification of risks and proposing of mitigating actions must always be done in light of the particular organisations' risk appetite.
- **Implementation of Defence in Depth strategy:** Once all risk areas have been identified and mitigation plans proposed, it is necessary to implement the proposed controls in such a way that it ensures optimum functionality of systems, the integration of controls across the organisation, as well as compliance with the overall business strategy and risk management process.
- **Maintenance, monitoring and review:** Due to the fast changing environment of IT, it is necessary to continuously monitor and review the functioning of the strategy, to adapt it to any changes in threats the organisation might face, changes to business goals or objectives or changes to the regulatory environment.

### **3.5 Layered Defence Approach as part of Defence in Depth Strategy**

Modern trends place increasing demands on information security within an organisation: users need remote access to the network, third parties have to access the organisation's network to perform certain functions or access specific information and more users within the organisation now need access to resources that were previously granted to a select group of users.

The most effective way to secure information within these parameters would be through implementing different layers of control as part of the Defence in Depth strategy (Murali et al., 2007). Tippet (2004) warned that "perfection in information security is impossible" and that smart people should zero in on identifying and building layered security controls around the network, because layering meant that even if one control failed, another was almost certain to catch the problem.

Webopedia defines a layered defence as multiple layers of protection. A layered defence means having multiple barriers to prevent attack, infiltration or malware infestation. These may include malware protection, possibly from multiple vendors, running at web and email gateways as well as on the desktop, firewalls at the network edge and on endpoints, intrusion detection, system intrusion detection systems and behavioural monitors, data leak prevention systems and a wealth of other possible defences, all operating in harmony to provide best-possible protection.

Controls will generally include both technical and process control mechanisms. Figure 3 provides a graphical representation of the layers of control implemented around a business process or key piece of business information (TISN, 2008):

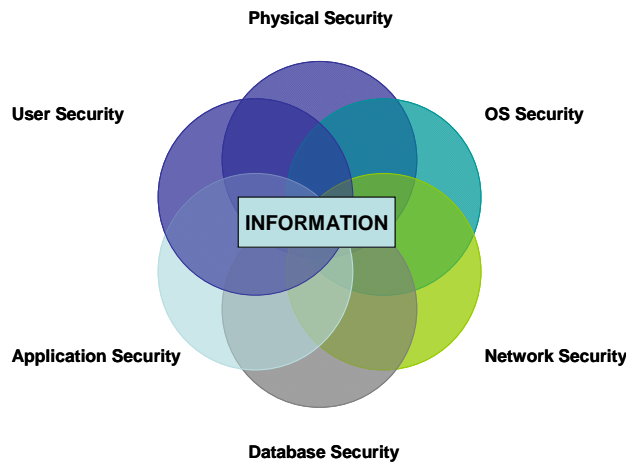


Figure 3: Layered Controls



Within the context of a Defence in Depth strategy a layered defence would mean that an organisation deploys multiple defence mechanisms between the attacker and the target. Each of the mechanisms must present its own unique obstacle to the attacker and must also include both protection and detection measures.

In practical terms it must increase the difficulty of successfully penetrating the network and thereby reducing risk, but also at the same time increase the chances of detecting the intruder:

- It must identify users of a system by means of passwords, user names, etc.
- It must also be able to provide for mechanisms to effectively and efficiently recover from damage caused by an attack.
- It must also be possible to correlate the results of information from various departments within a business and information from different controls, in an effort to increase business intelligence that can be used to identify and prevent future attacks and that can be shared within the market or with law enforcement agencies.

Within a broader context the concept of layered defence can also refer to the combined efforts of the public and private sector to combat cyber crime. The most powerful weapon available to fight cyber criminals is the very same asset they seek: information. Cyber criminals often rely on businesses, government and law enforcement not sharing any information or connecting random attacks to establish a *modus operandi*. They are often able to strike at different businesses within a same industry within a relative short period of time, because businesses are reluctant to share information about attacks with their counterparts. Although this is understandable seen in light of the fact that businesses might lose competitive advantage or market share, it is only the criminals that benefit from not sharing information about attacks.

However, the more developed the methods of information sharing between industry members, and between business and law enforcement agencies are, the less the need for a situation where full public disclosure will be called for.

### **3.6 Maintaining a Defence in Depth Strategy**

Maintaining a Defence in Depth strategy includes continuous monitoring and evaluation of the effectiveness of the implemented program. This would include evaluation the strategy to determine alignment where there are changes to the organisations' business objectives or the overall enterprise strategy, where there are changes in the security profile or specific breaches in security occur, where

there is an increase in particular security breach phenomena such as an increase in key loggers that are being detected throughout the industry, as well as when weaknesses or gaps that are identified within the current strategy.

The TISN (TISN, 2008) also recommends the model outline in Figure 4 to analyse the combined effectiveness of individual protection layers – whether currently in place or proposed for implementation. The effectiveness of these individual protection layers must then be considered within the context of the identified threat environment.

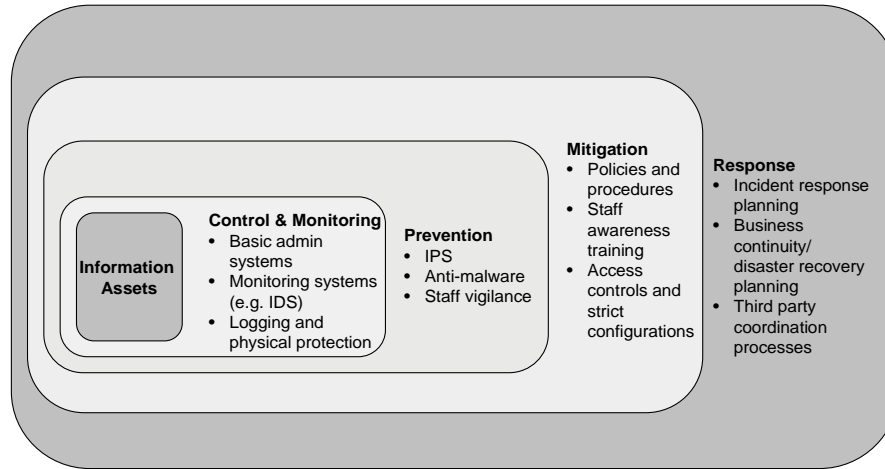


Figure 4: Layers of control protecting an information asset (TISN, 2008)

Practical guidelines for maintaining the strategy and improving on it where applicable can include the following:

- **Know and understand your organisation:** This includes an understanding of the external environment and the threats facing the organisation. It also refers to a thorough understanding of the internal environment and the way the organisation operates – its employees, levels of staff morale, business partners of the organisation, service providers, etc.
- **Define security roles and responsibilities:** Although security should be everyone within an organisation's concern, ownership of information security should be assigned to specific individuals, coupled with the necessary levels of authority and accountability. To

assist with the process it is recommended that security roles and responsibilities be incorporated into job description and that performance in terms of these areas be measured accordingly.

- **Adopt appropriate policies and procedures:** Once the Defence in Depth strategy has been drafted, the necessary policies and procedures should be put in place to govern the proper use of IT within the organisation, thereby ensuring optimal security. This would include updating policies and procedures as the need arises and to incorporate necessary changes in regulations, technology or operational requirements, as well as training and the creation of awareness with internal and external users. It is also critical to develop and define an appropriate incident response procedure and that this procedure is communicated to all users.
- **Continuous auditing and assessment of process:** It is recommended that a process of continuous auditing be implemented to ensure that the strategy remains aligned to business objectives, adapts to changes in technology or identified threats, and to allow for the analysis of information that is gathered from the different implemented controls.
- **Stay up to date:** Maintain awareness of new developments in both technology and services. Use a risk-based approach to determine when it would be necessary to upgrade or adapt current systems and processes to accommodate new developments.
- **Effective public private partnerships:** The effective control of cyber crime requires more than just cooperation between public and private security agencies. The role of the communications and IT industries in designing products that are resistant to crime and that facilitate detection and investigation is also of critical importance. To effectively address cyber crime also calls for a less re-active and more pro-active approach to the prevention, detection, investigation and prosecution of these crimes. Whilst it might be that only law enforcement can arrest criminals, service providers and private sector organisations can do much to investigate and prevent cyber crime (Forman, 2009). Within the context of a Defence in Depth strategy, such partnerships can deliver valuable business intelligence to prevent further attacks or to be able to detect them within an information system. Criminal intelligence analysis needs to be integrated fully into business intelligence, risk assessment needs to incorporate criminal threats, and cyber security needs to be conceptualised as part of a broader security problem that cannot be understood or dealt with in strictly technical terms (Williams, 2009).

#### **4. CONCLUSION**

In today's world information is fast becoming the most valuable asset an organisation has. Information underpins every strategy, system and business objective within an organisation and without ready and reliable access thereto, organisations cannot function on an optimal level.

It is however, critical to preserve the integrity of information, to ensure that it is stored, transmitted and accessed securely and that any system designed to manage and secure information is reliable, aligned to business objectives and in accordance with the risk management approach of the organisation.

Achieving Information Assurance in an organisation through the implementation of a Defence in Depth strategy poses significant benefits. It also ensures that South African organisations are aligned to the regulatory provisions contained in the ECT Act.

The shift in paradigm from a re-active to a pro-active approach and focusing on prevention rather than the prosecution of criminals that attack your system, poses benefits in terms of cost, time, resources and organisational reputation. The shift in paradigm required also includes to the need for sharing business (and criminal) intelligence and forming effective public private partnerships, reporting on threats and attacks and balancing what is best for the organisation with what is best for the community as a whole.

#### **ABOUT THE AUTHOR**

Jacqueline Fick is admitted as an advocate of the High Court and holds the degrees B Iuris, LL B and MBA. She has over twelve years experience as a prosecutor and was legal and strategic advisor to the Head of the Directorate of Special Operations for almost two years. She has presented papers at local and international conferences and is currently employed by PricewaterhouseCoopers in their Advisory Division.

## REFERENCES

1. Campana, J. (2006), Identity Theft: More than Account Fraud. What everyone should know (April 2006), <http://www.jcampana.com>, accessed on 16/02/2009
2. Foreman, M. (2009), Combating terrorist financing and other financial crimes through private sector partnerships, <http://www.emeraldinsight.com/1368-5201.htm>, accessed on 03/03/2009
3. Lüders, S (2006), A 'defence-in-depth' strategy to protect CERN's control systems (09/02/2009), <http://cerncourier.com/cws/article/cnl/24162>, accessed on 01/07/2009
4. Murali, D and Ramesh, C. (2007), Pseudo-intellectualisms continues to be attached to computer crimes, The Hindu, 04/07/2007, <http://www.thehindubusinessline.com/2007/07/05/99hdline.htm>, accessed on 15/06/2009
5. National Security Agency of the United States of America (NSA), Defence in Depth: A practical strategy for achieving Information Assurance in today's highly networked environments, (date published unknown), <http://www.nsa.gov/ia/files/support/defenceindepth.pdf>, accessed on 10/06/2009
6. Tippett, Peter (2004), Easy does it, (24/02/2004), <http://www.computertimes.asiaone.com.sg/people/story/0,5104,2021,00.html>, accessed on 01/07/2009
7. Trusted Information Sharing Network for Critical Infrastructure Protection (TISN) (2009), Defence in Depth: Summary Report for CIO's and CSO's, (June 2008), <http://www.tisn.gov.au>, accessed on 10/06/2009
8. Tung, L. (2009), Microsoft: Defence in Depth is not enough, (19/05/2008) <http://www.zdnet.com.au>, accessed on 12/06/2009
9. Wikipedia, (2009), Information Assurance, [http://en.wikipedia.org/wiki/Information\\_assurance](http://en.wikipedia.org/wiki/Information_assurance), accessed on 18/06/2009
10. Wikipedia, (2009), Defence in Depth, [http://en.wikipedia.org/wiki/defence\\_in\\_depth](http://en.wikipedia.org/wiki/defence_in_depth), accessed on 18/06/2009

11. Williams, P. (2009), Organised Crime and Cyber-crime: Implications for Business, <http://www.cert.org/archive/pdf/cybercrime-business.pdf>, accessed on 13/02/2009

