# *“Changing the value perception of security”*

By Desmond Ward

*“This project is submitted in partial fulfillment of the requirements for the MSc degree in information technology security of the University of Westminster*"

Supervisor Gavin Butler

Date of submission: September 2006

## Abstract

A recent report from Deloitte Touche Tohmatsu[1], illustrating the finding of its survey into the state of IT Security within the global financial services industry stated that *"Although the majority of respondents [Of the survey] are still doing poorly at measuring … the ones that do measure performance appear to be focusing more on cost and returns as opposed to the value the security provides to organizations. Evaluating security projects in terms of the value and impact delivered to the business and identifying a language that both security and IT people can talk, … will also result in projects that will become more aligned with the needs of the business."* This statement alludes to the fact that the value that security can provide to an organization is not being accurately illustrated and that measurement of the performance of the security function is not being conducted.

Research throughout the document provides a view of organisations placing great important on compliance, without attempting to understand the risks they face. These risks have been shown to be increasingly focussed on the internal sociological weakness within organisations, whilst the response from organisations focuses on external technological controls. This has been shown to provide a perception of security as a technical overhead rather than an organisational investment. In addition, measurement of security within organisations tends to focus on the performance of technology rather than the protection against threats, as research shows that there is a lack of confidence in the ability to provide protection against internal threats.

The intention of this document was to show that value and performance, as described above, of security functions can be exhibited to the enterprise through the utilisation of the Benefits Management[2] and SABSA®[3] methodologies amongst others. It is felt that utilisation of these techniques has sufficiently proven that value in non-financial terms can be shown and that the benefits of a well-structured security function are of great value to the future prosperity of business functions within the enterprise.

## Table of contents

# 1 Introduction

The purpose of this document is to discuss the value perception of security functions and related activities from the enterprise perspective. A recent report from Deloitte Touche Tohmatsu, published in 2005, illustrating the finding of its survey into the state of IT Security within the global financial services industry stated that *"Although the majority of respondents [Of the survey] are still doing poorly at measuring performance – if they are attempting it at all – the ones that do measure performance appear to be focusing more on cost and returns as opposed to the value the security provides to organizations. Evaluating security projects in terms of the value and impact delivered to the business and identifying a language that both security and IT people can talk, will not only help the security function achieve greater recognition but will also result in projects that will become more aligned with the needs of the business."* This statement alludes to the fact that the value that security can provide to an organization is not being accurately illustrated and that measurement of the performance of the security function is not being conducted.

If these statements are correct, then there is very real issue with regards to the ability of security functions to illustrate value. This is even more so in the light of the fact that the survey was directed to an industry that is undergoing an increasing period of regulation, with regulations such as Basel II[4] and Sarbanes-Oxley[5] gaining prominence at the boardroom level.

Research was undertaken to determine the validity of the above statement, consisting of reviewing the results of a number of surveys published during the past year (2005-2006) reading published literature deemed to be of note and searching through internet for sources of information. This allowed to compilation of this document as a result of the above research.

Prior to proceeding, it is deemed useful to try and define security, as the Deloitte survey alluded to their being a lack of commonality between the language of security and the enterprise. So what is security? Definitions for security from the Collins Concise Dictionary[6] that are deemed applicable include:

- *'The state of being secure'*
- *'Precautions taken to ensure against theft, espionage etc'*
- *'The protection of data to ensure that only authorised personnel have access to computer files'*

The above definitions lead to two further questions, what is 'being secure' and is security only related to data on computer files?

The definitions of secure[7] deemed relevant are:

- *'Free from danger, damage etc'*
- *'To make … safe from attack'*

As for the point relating to data, looking at the definition of data[8], we see the entry *'Also called Information'*. Looking at the definition of information[9], the following is observed:

- *'Knowledge acquired through experience or study'*

From the above exercise, even without proceeding to a specialist book on the subject of security we are lead to believe that security is an issue primarily for computer data if we were merely to look at the dictionary definition of secure.

However, as we delve deeper into the definitions, we can reasonably deduce that security is:

- *Being safe from danger, damage and attack (As security is the state of being secure)*
- *Taking precautions against theft, espionage etc*
- *The protection of computer data or information acquired through experience or study to ensure that only authorised personnel have access. (As data is also called information which in turn is knowledge acquired through experience or study).*

For the purposes of the remainder of this work, the precedent definitions shall be used when talking about security. All three definitions relate to a threat, whether it is of damage, attack, theft, espionage or access to data/information from unauthorised personnel. The issue facing organisations is to determine their susceptibility to being affected by the threat and what would happen if the threat were to affect them. These are also known as the vulnerability to exploitation and business impact. Combined with the severity of the threat, these assessments compose the risk posed by the threat. Risk is defined[10] as the *'possibility of incurring misfortune or loss'*. In order to determine this possibility, an understanding of the threats that could affect an organisation must occur.

The remainder of this report will attempt to determine if the Deloitte statement is correct, concentrating on the areas as follows:

- Current threats affecting the enterprise
- The current state of enterprise security
- improving the value perception to the enterprise
- Conclusion

# 2 Discussion on the current threats to the enterprise

This chapter will discuss the current threats to the enterprise. Deloitte stated that *"in order for an organisation to be in a position to provide effective information security, it must first have a clear focus on what it is seeking to protect and the corresponding threats. An understanding of these threats will dictate the processes and security technologies that will adequately protect, and be flexible enough to change with, the operating environment."*[11] The Basel II accord categorises the threats that organisations face as being in one of the following categories[12]:

- People
- Processes
- Systems
- External threats

With this in mind, we will now look at each area in detail to determine the ability of the security industry to protect against the threats posed by each category.

## 2.1 Threats posed by people

As external threats are covered in the fourth category, we shall restrict the discussion of the threats to those people who are within the logical perimeter of security provided by an organisational entity (Typically denoted by Firewall security devices, located on either the host or network infrastructure). This grouping is commonly termed the 'Insider threat'.

In a survey conducted by the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) [13], 68% of respondents reported that losses were deemed to be due to this so-called insider threat, with 39% of those feeling that the insider threat accounted for more than 20% of their total incidents.

So what threats can people pose? The Audit Commission's report into ICT Fraud and Abuse[14] categorizes incidents into the following categories:

- Fraud
- Theft
- Unlicensed software
- Private work
- Invasion Privacy
- Hacking
- Sabotage
- Virus
- Inappropriate material

Of those above, the greatest instances detected were Inappropriate Material (47%), Virus (16%) and Fraud (15.5%). Theft (Of information), hacking and sabotage combined made up less than 10% of all incidents detected. Of the total instances across all categories, 37% were conducted by operational staff, 31% by administrative/clerical staff and 15% by managers. This again is line with the CSI/FBI research, although a survey by CERT[15] suggests that 80% of internal attacks were conducted by people with technical knowledge of the infrastructure.

In order to better understand the threats posed by people, each of the categories will be discussed in more detail:

### 2.1.1 Fraud

The Audit Commission defines fraud as coming under one of the following headings[16]:

- *Unauthorised alteration of input*
- *Destroying, suppressing, or stealing output*
- *Making unapproved changes to stored information or*
- *Amending or misusing programs (Excluding virus infections)"*

Each of the above is further defined by Bainbridge[17]:

- *Unauthorised alteration of input*
  This is defined as the *"unauthorised alteration of data prior to in being input into a computer system"*[17]. The typical modus operandi of this particular threat, according to Bainbridge, is for a person to alter information prior to handing it to another person to enter into a computer system. This threat is deemed by Bainbridge to be easy to attempt as it requires *"no particular computer skills. The only intelligence required to succeed is in knowing the organisation's checking and auditing systems thoroughly and matching the fraud up with any shortcomings in those systems"*[17]

- *Destroying, suppressing, or stealing output*

  This motive for this fraud, according to Bainbridge, is *"usually to hide some criminal activity"*[18] by destroying output data from a system.

- *Making unapproved changes to stored information*

  Bainbridge makes the distinction between this type of fraud and the unauthorised alteration of input in that *"it is the person entering the data into the computer that makes changes to the data"* [19]. He goes further to state *"Most organisations using computers are vulnerable to fraud perpetrated by employees preparing data for entry into a computer."* [20]

- *Amending or misusing programs (Excluding virus infections)*

  This fraud relates to the deliberate utilisation of a computer program to facilitate fraud. This can either be done to utilise a configuration weakness in a program or insert a function within the object/source code of a program to conduct fraud. Bainbridge states that this *"is much harder to detect than data fraud"*[21] and that staff *"involved in the commissioning or alteration of software present another source of danger in that many of them will have detailed knowledge about the security and password systems used"*. [22]

### 2.1.2 Theft (Of information)

The Audit Commission report states that it has not included the theft of equipment due to it being *"easily replaced and insurable"* [23]. The report concerns itself with the theft of information as it *"may well cause embarrassment, loss of confidence and potentially business disruption or even failure"*. Actions under this category are therefore understood to be the theft of personal data as defined under the Data Protection Act 1998[24] (DPA 1998) or intellectual property. We will look at the issues surrounding the theft of either type of information in turn.

The seventh principle of the DPA 1998 states that *"appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*[25] This obligation is applicable as the definition of personal data is *"data which relate to a living individual who can be identified …from those data and other information which is in the possession of, or likely to come into the possession of, the data controller"*.[26] This clearly places an obligation on companies to take steps to ensure that theft of personal data cannot occur. Notwithstanding the legal obligations, a study[27] showed that on average, the affect to an organisation after information leakage was a 5% drop in share price, 19% loss of customers and 58% loss of customer trust.

The threat of corporate espionage is becoming more relevant with recent examples being discussed in the section on external threats, and a study from McAfee[28] finding that 21% of workers let friends and family use their systems to access the internet shows the potential for information leakage. When you add this to the high profile loss of portable devices such as laptops, there is a very real opportunity to provide information to other organisations due to mistakes. As information can often provide competitive advantage, people can also be coerced into divulging information, either whilst in employment or afterwards. In response to information disclosure relating to a government document in 2005, a security specialist stated[29] that their *"research shows that up to 75% of business documents can contain sensitive information most people would not want exposed, with a further 90% having no idea that confidential information was being leaked"*.

Recent attacks on organisations such as Sumitomo Mitsui bank[30], show that criminal elements are actively using the fact that organisations don't conduct adequate endpoint security and allow the least vetted employees (eg Cleaning staff) the most access to the building. Endpoint security is becoming more important as a result of this, with the lack of vetting relating to PS/2 and/or USB ports on computers/servers and the threat of corporate data theft becoming more real due to the proliferation of high-capacity portable media, both on portable music players and the capacity of storage media in mobile communication devices. Indeed a recent study[31] showed that out of twenty USB drives placed within the campus of an American

Financial Institution, fifteen were picked up by employees and subsequently connected into the computer systems belonging to the organisation. The USB drives contained a program masquerading as an image file which collected login credentials and other information

### 2.1.3 Unlicensed software

The Audit commission report restricts the issue of employees using unlicensed software to that of the arena covered by the Copyright, Designs and Patents Act 1988[32]. However, the threat to an organisation is more than the legislative penalty under the realm of intellectual property. As shall be illustrated throughout this document, a lack of control over what applications are installed can assist criminal elements in their activity; create weaknesses in infrastructure by not being able to identify and install security patches and assist employees in the conduction of criminal activity.

### 2.1.4 Private work

The utilisation of corporate systems for non-work purposes could place the corporate information at threat. The threats discussed within this section could all apply in the event of an employee conducting this activity.

### 2.1.5 Invasion (Of) Privacy

This category relates to the breaches of the DPA 1998 legislation. The implications relating to a failure in the security of personal data has already been discussed in this

document, but another issue is the lack of control over the utilisation of personal data within an organisation. A recent report**XX** has stated that organisations are using personal data in breach of the second principle of the DPA 1998 whereby *"Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes"*.[33] The utilisation of live personal data within non-production systems is deemed to be prevalent within this report. This again can place organisations liable to prosecution from the Information Commissioner.

### 2.1.6 Hacking

The Audit commission appears to have restricted it's definition of hacking to the external attacks, as it states that the respondents had installed access control software and firewalls to help minimise unauthorised activity[34]. As shall be illustrated within this report, the assumption that hacking activity will predominantly be mounted from the exterior of the traditional network perimeter is a flawed one.

Over 2003 to 2004, there has been an increase in the availability of security testing tools, like the Nessus vulnerability assessment tool[35] and the Metasploit framework[36]. These suites of tools, which began life within the more unknown Unix-type operating environments, are rapidly becoming available to the mainstream windows platforms; although intended for security-testing purposes, these suites are readily available for anyone with a little knowledge to be able to launch attacks against other

systems. In the case of the Metasploit framework, the operating environment is very intuitive and additional exploits are being made available dynamically. This increases the amount of potential attackers and their associated capability without requiring additional technical knowledge.

### 2.1.7 Sabotage

The commission concentrates on physical attack/damage and cyber-vandalism (ie Spam and phishing) [37] as the forms of sabotage encountered. Within this definition, the commission feels that the survey results suggest that there are weak controls surrounding access to internal ICT and management of disgruntled workers. The latter points would appear to allude to the internal hacking threat although this will be developed further in other sections.

### 2.1.8 Virus

Whilst it is certainly true that examples such as the attempted theft from Sumitomo Mitsui in 2005 show the threat that can be posed by malicious employees, not all attacks mounted from within the enterprise are consciously committed by affected employees. Viral attacks are deemed to cause medium to high business disruption to 42% of respondents to the Audit Commission report[38], and the Department of Trade and Industry (dti) additionally stated in their Information Security Breaches Survey 2006[39] that 83% of very large businesses had a malicious code infection, compared with 43% for large businesses and 35%

overall. This is despite 98% of businesses deploying anti-virus software and 74% using anti-spyware solutions[40].

The commission report interestingly stated that all respondents to their survey *"replied that they used virus prevention software and yet the primary reason for virus infections was seen to be ineffective virus protection facilities"*.[41] Given recent developments with so-called 'Spyware', and the examples given within this document then this statement appears to be correct; the dti additionally stated in their survey that 25% of UK businesses were not protected against Spyware[42].

This can, in part be blamed on the failure of specialist anti-virus companies from blocking programs which have a 'legitimate use', however an ideal example of the failure of this policy is seen when Sophos refused to block the Coulomb dialler software used to access pornographic websites[43]. As Sophos have no software targeted for the home use market, it has to be said that the likelihood of such dialler software having legitimate use within an organisation using their protection software is questionable.

However, when looking at the analysis of the top ten viruses from Sophos in Appendix I, we can see that the most successful malware from an infection standpoint over the past three years is the Netsky[44] and Zafi[45] families, with the Mytob[46]/Sober[47] variants also in prominence. What is the reason behind the success of these variants? An analysis of the variants reported shows that they all have a mass mailer element, all attempt to stop security products

from running and harvest email addresses from the infected systems, they all use some form of social engineering to get the victim to run an attached file and all attempt to slow detection by not sending emails to security sites.

The simple fact appears to be that people continue to click on unsolicited attachments via email. A study conducted by Trend Micro[48] showed that 63% of respondents stated that they were more comfortable clicking on suspicious links or visiting suspicious websites because the IT department has installed security software on their machine. 39% of the same respondents felt that the IT department will prevent them from falling victim to threats including spyware and phishing, a perception which encourages bolder online behaviour in many users. Within the same survey a percentage of those surveyed admitted that they were more likely to open suspicious emails or weblinks on their work computer than at home and said that it was because support was available if something malicious occurred; this figure ranged from 49% within the US to 28% within Japan.

This is reinforced by the fact that, since Sasser[49], none of the top three viruses detected since 2004 has needed to use any form of vulnerability to infect systems. Interestingly there have also been further reports[50] of a reduction in the amount of emails with viral attachments, with an increase observed in URL obfuscation techniques whereby the true destination is obscured from the victim in an email appearing to come from an trusted organisation to induce the victim to trust the content of the email and take them to a malicious website. Most of this type of fraud detected is

now believed[51] to relate to the online auction site ebay and/or it's subsidiary payment company PayPal. The rationale for the increased emphasis on gathering email addresses and the mass mailing elements observed within the most virulent malware will be discussed in later sections of this chapter.

Given that a recent study[52] by Harvard University showed that 90% of people studied failed to detect websites known to be utilised in the process of phishing, it is of little surprise that the above attacks are attempted.

### 2.1.9 Inappropriate material

This category constituted by far the greatest amount of incidents detected by the respondents to the Audit Commission report[53], constituting some 47% of the incidents detected.

Whilst personal utilisation of corporate resources is not forbidden by law, it certainly can bring both the employee and employer into breach of various laws. The main breaches in this instance would appear to be in relation to the Obscene Publications Act 1959[54], the Copyright, Designs and Patents Act 1988 and the seventh principle of the DPA 1998.

The ramifications of commiting an offence under the section one of the Protection of Children Act 1978[55] are that any system containing said images will have to be removed to be forensically investigated by law enforcement agencies.

This is without regard as to the purpose of the system, which could be a file server or even the only location of business-critical information. The impact of this could, therefore be detrimental to the business interests of companies.

Notwithstanding the nature of the images, unless the images have been created by the person possessing them, they may be either copyright or malicious in nature. In the first instance, mere knowledge of the contravention is enough to cause liability to companies under the Copyright, Designs and Patents Act 1988. The second instance is not a strict liability, but upon the compromise by any number of graphics files that can exploit vulnerabilities in different components host operating system and/or or resident applications, security measures can be circumvented and personal data disclosed. If this disclosure were to be traced to access to inappropriate content that a responsible person would expect a corporate entity to block, then this could lead to litigation as a breach under the seventh principle of the DPA 1998.

## 2.2 Threats posed by weakness in process

As can be seen within this chapter, the threats relevant to organisations are wide and varied. Some can be detected by technological means, but others cannot either due to the amount of data to be processed (In the event of positive event logging) or due to a lack of appropriate technical means (Also known as 'Out of bounds' checking. An example of this is the use of hardware keyloggers in the Sumitomo incident previously mentioned) to detect the measures

employed to execute the threat. The dti report illustrates this[56] by showing that only 49% of organisations conduct a periodic audit of their policies, 49% monitored activity and logged unusual events and 38% deployed software to detect, react and record policy violations.

In order to counter the threat posed by people, as illustrated above; processes are required to influence the behaviour of those people. Often, the need for control over the behaviour of people is not merely a desirable activity, but is an obligation either by law or regulation. Yet only 45% of financial services companies within EMEA provided their employees with a training and awareness programme on security and privacy issues during the last twelve months[57]. This section shall discuss the typical areas where companies can potentially expose themselves to either litigation or an inability to detect the activity within their organisations.

### 2.2.1 Audit policy

Despite the wealth of criminal law governing the protection of intellectual property, computer fraud and misuse of computers, this is all ineffectual unless an audit trail can be created and unauthorised behaviour defined by policy. Given the internal threat highlighted in the preceding section, it is important to monitor unauthorised activity relating to system and/or applications.

One of the common failings within companies is the lack of definition of what is authorised in terms of policy. The Computer Misuse Act 1990 (CMA 1990)[58], places great emphasis on unauthorised access in both parts one and two. Part one concerns the unauthorised access to a

computer system and part two builds on said access adding the *"intent to commit of facilitate the commission of further offences"*. Without some notification upon access to networked systems from internal employees that unauthorised activity is prohibited, it can be argued that unless financial fraud is being committed or the person is acting in conjunction with others (ie Where a conspiracy offence could apply) it could prove difficult to gain a prosecution.

In order to mitigate against computer fraud and other malicious utilisation of systems, it is recommended that computer systems be configured to log all failed access attempts and prevent access in the event that activity is detected that would normally be indicative of an attempt to subvert authorisation mechanisms. Financial applications should be configured to log sufficient information to provide an audit trail of activity within the application, in order to assist in the detection of fraud.

It is additionally recommended that all ingress points for applications and/or systems (eg Logon screens and/or Telnet/SSH prompts) be configured to state that unauthorised access as defined by IT Policy and parts one and two of the CMA 1990 is strictly prohibited and IT policy be amended to include guidance on what is authorised access. It is also best practice to introduce Role-Based Access Control and reduce the amount of shared login accounts in use to improve audit of activity and prevent excessive access.

### 2.2.2 Intellectual property policy

Given that only 56% of respondents to the Audit Commission report stated that they had been required to sign a confidentiality agreement as part of their conditions of service[59], the lack of adequate policies in this area can provide issues to organisations. One of the major issues with regards to theft of confidential information is that without express terms governing confidential information within an employee's contract, terms will be implied on an employee. Typical terms to be implied were laid out by case law during the ruling of the court of appeal in the case of Faccenda Chicken Ltd v Fowler[60]. The following was stated by the court:

- *"If there is a contract of employment, the employee's obligations were to be determined from the contract.*
- *If there were no express terms, the employee's obligations would be implied.*
- *While still in employment, there was an implied term imposing a duty of good faith. This duty might vary according to the nature of the contract of employment but would be broken if the employee copied or deliberately memorised a list of customers.*
- *The implied term imposing an obligation on the employee after the termination of his employment was more restricted. It might cover secret processes and trade secrets.*
- *Whether information fell within this implied term to prevent its use or disclosure by an ex-employee depended on the circumstances, and attention*

*should be given to the following:*

- *The nature of the employment;*
- *The nature of the information;*
- *Whether the employer stressed the confidential nature of the material;*
- *Whether the information could be easily isolated from other material the employee was free to use."*

The above would appear to provide direction that without a term in the contract covering confidential information, and ensuring communication to employees relating to the sensitivity of such material, that protection would be limited in the event of an employee leaving or being able to plead ignorance as to the nature of the material that he/she divulges.

It is recommended that companies implement an information classification process, which includes communication regarding the status of all material deemed to be confidential in nature to those employees who have access to said material. It is also essential that this communication is given to all third parties that would have access and ensure that terms are inserted within all contractual agreements relating to employees and third parties. The step regarding communication and contractual terms towards third parties is important as there is case law[61] that supports that notion that technological measures (eg Encryption) are not sufficient to imply an obligation of confidence.

### 2.2.3 Acceptable use policy

Due to the potential ramifications of allowing access to pornographic websites, as discussed in the preceding section, it is recommended that a policy be implemented that defines what consists acceptable use of the internet access provided and communicate this policy to all employees. This is even more important given that 60% of businesses who responded to the dti survey[62] stated that they did not block access to *'inappropriate'* websites, and only a sixth scanned outgoing emails for inappropriate content.

The definition of what constitutes acceptable use is becoming more important with 51% of people surveyed for McAfee[63] admitting to connecting their portable devices to their work PC and 60% storing personal content on their work PC. With 10% also admitting to downloading content at work they shouldn't, the issue is very real. Acceptable use policies should include the use of removable media, such as Personal Digital Assistants (PDAs), mobile phones and music players.

A final issue with regards to ensuring that employees understand what is deemed acceptable behaviour is that within the UK, the *'Multiple publication rule'*[64] applies, whereby every instance of a defamatory statement is taken into account. Under the Defamation Act 1996[65], the conduit for such statements would not be liable unless the organisation was made aware and took no action to remove the statement or stop its distribution. It should also be

stated at this time that it only takes two separate instances to constitute an offence under the protection from Harassment Act 1997[66], and companies should be aware of this too in a similar vein to the publisher's defence discussed above.

### 2.2.4 Encryption policy

When employees use encryption, it can be deemed that the only risk is that it is their issue and nothing of concern to corporations. However, obligations under the Part III of the Regulation of Investigatory Power Act 2000[67] (RIPA 2000) should be understood in this regard. Part III of the RIPA stipulates that if a person is in possession of *"protected information"* (i.e. electronic information seized or intercepted under the RIPA), an *"authorised person"* (such as law enforcement or intelligence officials, or a circuit judge) can serve a disclosure notice on that person, demanding disclosure of the encryption key or the document in unencrypted, intelligible form (Also know as 'the plaintext').

The notice must contain prescribed details, and it can only be served if specified grounds are satisfied. Failure to comply with such a disclosure notice could lead to up to two years imprisonment or a fine. In the event of a number of employees of a company potentially having access to the encryption key used, then the notice will be served to a senior officer of the company. It is of note that by ensuring that centralised encryption is implemented, the disclosure notice will be presented to the managerial functions of the

company, ensuring that the plaintext can be supplied and equipment will not always have to be removed.

### 2.2.5 Data Protection policy

The lack of understanding of data retention policy could have the potential to bring companies in breach of the fifth principle of the Data Protection Act 1998 (DPA 1998)[68], whereby *"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes"*. This would appear to be a major concern in the event of companies processing personal data as part of their commercial activities, with only 56% of respondents to the 2006 Deliotte security survey having a programme for managing privacy compliance[69].

As can be seen by the examples in the preceding section, there is an inherent risk in the event of a lack of understanding of the obligations under the data protection act on companies as a Data Controller. The breaches could result in companies not being allowed to process personal data, which would cease the ability to trade from e-Commerce sites and receive unlimited monetary penalties, proportionate to the distress and/or damage caused to those data subjects about which personal data has been disclosed.

The most relevant breaches highlighted within this document are of the fifth and seventh principles. However, the potential to be in breach of the second principle

whereby *"Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes"* is relevant where live personal data is used within non-production systems.

The following steps are recommended to provide compliance with the principles:

- Ensure that all processes are amended to ensure compliance with the DPA 1998 with regard to retention and processing of data
- Provide communication and training to those employees that process personal data
- Conduct security reviews as mentioned above on systems where personal data is stored/accessed
- Ensure that a policy exists providing the process to follow in the event of subject access requests, and detail an audit procedure to verify this process
- Ensure that e-Commerce websites and applications have a tick box as part of the license agreement/registration page to satisfy the requirements of the DPA 1998 with regards to informing data subjects as to the processing of personal data
- Nominate an individual to have the responsibility for keeping abreast of changes in the DPA regulations

### 2.2.6 Application development policy

With the threat posed by configuration weaknesses and

vulnerabilities in both applications and systems discussed within the next sections of this chapter, companies need to take steps against the threat posed to their environment. It is tempting to rely on legislative measures to protect against these threats. Whilst it is true that hacking is covered under part one of the CMA 1990, it is unwise to rely on this legislation to focus the onus of responsibility onto the attacker. There is a need to ensure that web applications are fully tested to prevent disclosure of information unless the correct authorisation mechanism has been complied with.

This is not only important with regards to pursuing punitive measures against attackers, but is also an obligation under the DPA 1998, the Payment Card Industry (PCI) Data Security Standard[70], and the Supply of Goods and Services Act 1982[71].

The PCI guidelines consist of twelve requirements that cover the majority of security best practice. The guidelines were to be adopted by any entity processing credit card payments by 30 June 2005, with a maximum fine of $500,000 in the event or a system compromise due to non-compliance with the guidelines and $100,000 for each incident whereby card data may have been disclosed and VISA has not been informed[72].

In addition to this, section thirteen of the Supply of Goods and Services Act 1982 implies a term into any contractual agreement that the supplier of a service (Which will be the case unless selling something to a consumer) *"will carry out*

*the service with reasonable care and skill"*. This implication will only be exempted if a term is inserted into contractual agreements between companies and their customers.

All of the above show that not only is it desirable to take such steps to secure e-Commerce sites, it is an obligation that companies can ill afford to ignore. The punitive steps that can be taken against companies with regards to disclosure of personal information and credit card details, are severe and not to be ignored..

It is therefore recommended that companies undertake steps to comply with the PCI requirements and review their websites according to the Open Source Web Application Security Project (OWASP)[73] and/or Web Application Security Consortium (WASC)[74] guidelines through security assessment of the hosted applications.

### 2.2.7 Monitoring policy

The monitoring of emails and files gives concern within companies, due to the lack of terms within either policy or employment contract governing such activity within companies.

Monitoring of email communications is allowed under *'The Employment Practices Data Protection Code Part 3 Monitoring at work'*[75] where monitoring that causes *"any adverse impact on workers is justified by the benefits to the employer and others"* (Adverse impact refers to anything about the employee that *"May intrude into their private*

*lives"*). As this is hard to fully define, the only obligation appears to be that the monitoring is justified. The act further states that monitoring can consist of *"Randomly opening up individual workers' emails …to look for evidence of malpractice"* and *"Using automated checking software to collect information about workers, for example to find out whether particular workers are sending or receiving inappropriate emails"*. However, Article eight of the Human Rights Act 1998 (HRA 1998)[76], states that *"Everyone has the right for his private and family life, his home and his correspondence"*.

The terms above would appear to indicate that as long as monitoring takes the form of random manual access and/or automatic collection then that would be permitted. It would be inferred from the above, however, that selective access not designed to look for malpractice would be a direct contravention of Article eight of the HRA 1998.

Monitoring should be addressed within companies by a definition of what will be monitored to be entered into the IT Usage Policy and communicated in the login prompts to access corporate systems in conjunction with notification of the fact that monitoring will take place. All monitoring activities are recommended to be automatically collected with access to the content of files and/or communications (Internet or email) requiring a request from a manager, or above, by means of a form signed by the Human Resources department. IT Security functions should have the right of audit of all systems used to collect such information to ensure that access to employee's data and/or

communication is in line with best practice under both the Data Protection and Human Rights Acts as discussed previously.

### 2.2.8 Incident response policy

It is unlikely that organisations will be fully aware of security breaches given that research within the Audit Commission report showed only 32% of respondents knew where to find documented procedures for reporting a security incident.[77] This lack of communication or even presence of a defined incident response policy can result in an inability to prosecute malicious people due to not handling the evidence to the best practice guidelines set by the Association of Chief Police Officers (ACPO). [78] There is a very real danger that without a clearly defined and communicated policy in this regard that security functions will be unaware of intrusions until days or even weeks after the event, by which time the attacker may have had the opportunity to increase the damage inflicted on the enterprise. The ability of the enterprise to accurately undertake corporate governance may also be affected, due to a lack of understanding with regard to the incidents within an organisation. Given the obligations previously mentioned with regards to the PCI guidelines etc, it is imperative that all risks are adequately understood.

## 2.3 Threats posed to systems

Vulnerabilities and configuration weaknesses in operating systems and applications have posed a threat to organisations for a number of years. There are numerous high-profile examples of the effects of exploitation of these weaknesses, with the 'Severe disruption' to UK Coastguard computer systems[79] caused by a worm exploiting an vulnerability in the Microsoft Windows operating system being a prime example of the impact that can occur. The worm caused severe disruption at all 19 stations and the headquarters, including mapping systems; this caused the staff to revert to using manual processes to continue their work, which included using paper maps.

A recent report from the SANS institute[80] has highlighted the following trends:

- Critical client-side Windows vulnerabilities are on the increase, whilst service-based vulnerabilities are on the decline.
- So called 'Zero day' vulnerabilities are on the increase within Microsoft Internet Explorer
- There is an exponential growth in critical vulnerabilities affecting databases and other data-warehousing systems
- Attackers are increasingly targeting endpoint security solutions such as anti-virus

When this is combined with the following points from the recent Symantec Threat Report[81], the threat posed by vulnerabilities is increasing:

- 1896 vulnerabilities were observed during 2005, the highest total since 1998 and 40% more than 2004

- 79% of vulnerabilities during 2005 were classed as being easy to exploit

The time to exploit these vulnerabilities is also shortening due to the emergence of reverse engineering of security patches to discover the original weakness.

A study of the Microsoft vulnerabilities released between 2003 and 2006 has been conducted in Appendix II, categorising the vulnerabilities to provide a statistical analysis. This analysis allows the vulnerabilities to be graded according to the component affected and the likelihood of exploitation.

The amount of exploitation that requires end user interaction has risen considerably from 55.6% in 2003 to 86.9 to date in 2006, with a corresponding rise within critical vulnerabilities within applications from 26.2% to 82.5% within the same period. With application vulnerabilities overtaking operating system vulnerabilities for the first time since 2002, and the ratio of critical vulnerabilities requiring user interaction continuing to rise compared to correspondent wormable vulnerabilities, this would show a rationale for the prevalence of viral code utilising social engineering to provide a means of exploitation. In many cases, this user interaction can be nothing more than visiting a site to become infected. It is of also of note that as from MS05-012[82], the OLE/COM vulnerability on Microsoft Exchange 5.5 running on the Windows NT4.0 operating systems was only available through paid for premium support. This is the first known time that Microsoft refused to provide a free security patch for an affected system, which on Exchange would be considered wormable. This is of interest with support for Service Pack One of the Windows XP operating system ceasing from 10th October 2006[83].

In 2005, a security company[84] connected six computers - with six operating systems - to the Internet for a week without any virus protection. The results returned 4892 direct attacks by viruses, worms and other types of malicious code, and 46255 scans by remote computers looking for weaknesses. Windows XP Service Pack One was attacked 4857 times, and successful attacks occurred within 18 minutes by the Blaster and Sasser worms. Within an hour, the computer was taken over and began attacking other Windows machines. All the other operating systems. including various versions of Linux, Apple Mac OS X and Windows XP Service Pack Two, survived the attacks which combined amounted to 35 attempts.

Due to the increased reliance on the interaction of end users to facilitate the exploitation of vulnerabilities, a number of different methods have been employed. We shall now discuss three different examples to highlight these different methods.

- During 2005 it was reported that links to unsubscribe from spam email lead to a website utilising the "Drag 'n' Drop" [85] vulnerability to install software onto unsuspecting victim's machines.
- Programs were installed using the overflow vulnerability[86] in Microsoft's GDIplus JPEG processing mechanism. This incident was noted thirteen days after the associated Microsoft bulletin was produced, the patching for which was very complex due to the range of system and applications that it affected. This threat vector has been repeated using numerous graphic processing vulnerabilities during the second half of 2005 and throughout 2006.

- The infamous Jscob/Download.ject exploit[87] used vulnerabilities in the Windows Shell, adodb.stream ActiveX control and Help and Support centre to provide a bypass of Internet Explorer security. Code was uploaded to various websites to aid infection. This is one of the most prominent examples of the blended threats.

The problems that the "GDIplus" and "Drag 'n' drop" examples pose are the use of programs that may not be developed with malicious intent, but they are being used by malicious people for nefarious purpose.

Whilst wormable vulnerabilities can, in the main, be prevented by the use of best practices on the network perimeter, the higher ratio of vulnerabilities reliant on the email and/or internet browsing vectors necessitates the bypassing of standard security measures such as firewalls and moves the perimeter to be secured to the actual desktop. One of the most surprising statistics recently, is the determination that 50,000 new hosts were harvested into roBot Networks (Botnets) using the vulnerability within the Server service, patched in MS06-040[88]. This is surprising as the exploit used relied on the ability to communicate across TCP ports 135 and 445, which were blocked by most organisations after the Sasser and Blaster worms, and would appear to indicate that standard firewalling best practice is not being universally followed. Given the advent of so called 'fuzzing'[89] techniques that are designed to find vulnerabilities by using large amounts of data designed to detect error conditions within software, it is believed that the amount of vulnerabilities will increase. This is supported by examples such as the daily publication of a vulnerability within an internet browser undertaken during July 2006 by the creator of the Metasploit exploitation framework[90].

These threats are not confined to Microsoft products however. The SANS *'Top 20 Critical Internet Security Vulnerabilities'*[91] provide an illustration that Unix systems, Network systems (Including perimeter security devices) and applications all present items of concern to organisations connecting to the internet. Issues range from vulnerabilities to configuration weaknesses.

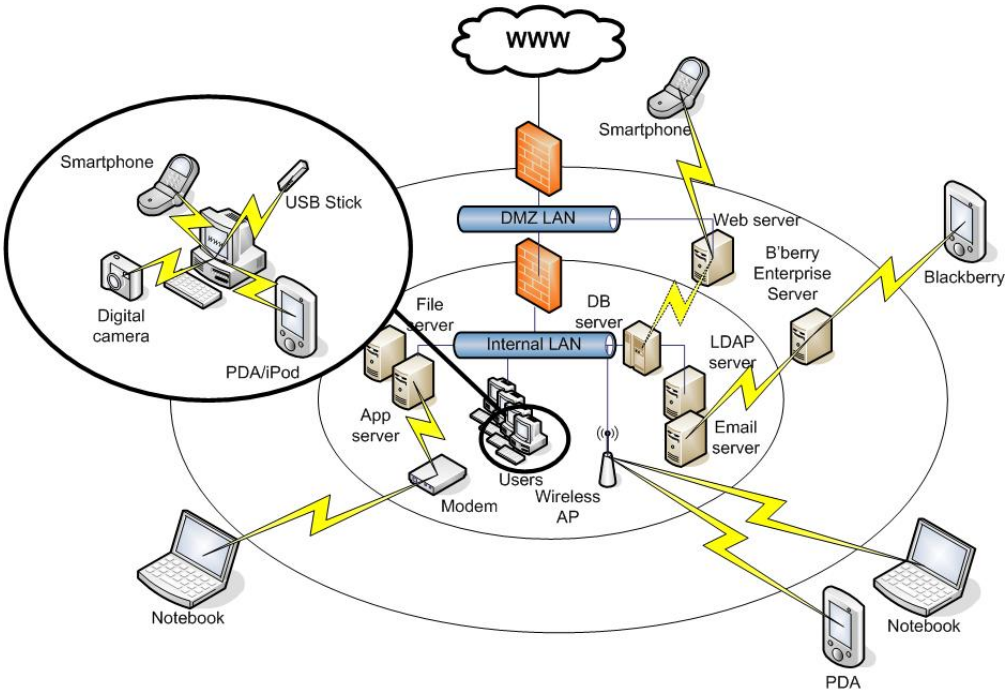
In addition to this, the long-held paradigm of perimeter security has been shattered; this is due to the increase in vulnerabilities over essential services that have to be open across the internet (eg Internet traffic traversing over TCP ports 80 and 443). Firewall technology has now reached a level where they are capable of thwarting all attacks that they are configured for, but still have to allow such services access to and from the internet. However, as is discussed within the next section, the amount of interconnection between different companies is also posing an issue for organisations where an infection within one organisation can easily spread if not controlled. Commandment three of the Jericho Forum commandments[92] states that assuming the context in terms of the placement of a system is unwise as the *'Security solutions designed for one environment may not be transferable to work in another. Thus it is important to understand the limitations of any security solution'*.

## 2.4 Threats posed by external entities

This section will discuss the threats that originate from outside the corporate network perimeter. With 53% of all respondents to the dti security survey reporting that they have outsourced some of their IT operations[93] and the increase in the sharing of information between organisations, the perimeter of the network is becoming weakened.

This is also evident when looking at the example infrastructure in figure 2-1 below.

The systems used to host information and conduct business are now extending onto mobile communications devices, such as Smartphones and Laptops. This is resulting in the access to corporate applications/information being required outside of the trusted internal network to a environment where the end user is responsible for the security of the information presented on the device.




Whilst 60% of respondents to the dti survey reported[94] that they implemented additional passwords above the normal network logon, 84% of these had not moved to a stronger form of authentications due to there being no business requirement. Only 8% of all respondents had implemented two factor authentication, and 60% had not adopted a Virtual Private Network (VPN) to protect the communications.

This lack of strong authentication is more relevant due to advisories from Messagelabs[95] and the National Infrastructure Security Co-ordination Centre (NISCC)[96] that have highlighted the threat posed from targeted email attacks where Microsoft Office files were observed as having malicious programmes inserted inside them. These organisations have reported a 600% increase over the past year, with 69% exploiting vulnerabilities within Microsoft Word. It was observed that in some cases, the time between the release of the documents onto websites that would be of interest to the target audience and the malicious programmes being inserted into them was as short as two hours and in certain cases, as few as seventeen people were being targeted within organisations[97]. This type of activity has also been evident in a recent case of industrial espionage where an Israeli couple were found guilty of using customised malicious programmes, including software keyloggers, to steal confidential information[98]. It should be noted that in the case of the industrial espionage, it believed that £17,000 was being paid per affected system per month[99]; this gives an idea of the financial incentive to conduct such activity.

Not withstanding the threats posed by such attacks, companies are not changing the way that they protect their systems, with 56% relying on the physical security of the premises alone and only 13% protecting hard drives by encryption or a password[100]. With recent reports showing that thousands of portable devices such as PDAs, mobile phones and laptops are being found in taxis in London alone[101], the threat from information theft and entry to companies is significant.

Of those companies that have outsourced IT operations, only 43% restrict the systems and data that outsourced personnel can access and 62% prefer merely to address data protection issues within a contractual agreement[102]. Given the example of the infection of the

UK Coastguard in the previous section, there is a very real danger from allowing unrestricted access between companies. If 57% of companies do not restrict network access to systems for another company, it even less likely those organisations will use network segmentation between different geographical locations of their own company. Returning to the above example relating to loss of portable devices, examples of information disclosure from the loss of a laptop such as those from Ernst & Young[103] (Disclosure of IBM, Sun, Cisco, BP and Nokia employees) and Fidelity[104] (Disclosure of 260 000 HP employee's details) show that companies also need to understand the security mechanisms that their partners take.

The corporate website often provides a portal to access information, and recent Gartner research has shown that 75% of all hacks occur at the application level[105]. The interfaces to allow the public to access these portals must, by design, be publicly available. eCommerce applications that access database back office systems such as Oracle and Microsoft SQL Server can allow unauthorised access to information and hosting systems if applications do not take adequate measures to protect against these attacks. The CSI report showed that 59% of respondents to their survey had experienced more than ten incidents against their website over the past year[106]. 89% of all corporate websites are externally hosted according to the dti survey[107], but only 29% of the respondents were aware of the security controls that the external hosting company employs with regards to their website.

The final threat to be considered in the realm of perimeter security is the proliferation of insecure wireless network Access Points (APs) within the enterprise. A recent study[108] of 2000 wireless networks shows that 62% are not encrypted, 99% do not hide their SSID. Of

those that do not hide their SSID, 70% provide information within the SSID to determine which company the network belongs to. This vulnerability is very real, and again shows the need for proper consideration in the planning of network and systems infrastructure within the corporate environment. The so called 'evil twin' scenario[109] should also be discussed at this point too, as even if a secure wireless network is implemented a breach can occur if the AP can be spoofed to coerce wireless systems to connect to it.

The increased penetration of residential high-speed connections to the internet is continuing, with 73% of all internet connections within the UK now using high speed connections[110]. ISPs are taking steps to improve the security of the scanning of emails and internet traffic, but they are limited in finding a balance between the provision of adequate security and preventing people from using the internet connection without restriction. This is evident in the recent reports of 50,000 new hosts being gathered into botnets due to the vulnerability within MS06-040. As has been previously discussed, the most prevalent malware in circulation all harvest email addresses, they send emails out and there is marked decrease reported in the amount of malicious attachments and a correspondent increase in phishing techniques being employed to circumvent security software. Recent studies[111] now show that the security software provided by the most well known companies are being used to test malicious programs against prior to release into the internet. This is resulting in a slow response to the viral threat from the main vendors, indeed recent research shows that in case of the Nyxem worm[112], it took up to four hours for the largest anti-virus vendors to provide protection against the methods employed. This gives a potentially window for external attackers to gain access to internal systems where the network controls are often weaker.

Organised crime in Denmark, Portugal, Romania, the UK and Russia have been reported to be moving to the internet, with reports stating that *"In the last two years cybercrime has become less open to 'ordinary' criminals like hackers as criminal organisations have started to realise the potentially huge financial gains to be made from the internet"* [113].

The financial incentive behind this activity is evident, with $2,500 being offered for the information from a thousand-node botnet[114] and botnets are being reported as being hired for $100 per hour by criminal elements, suspected to be from Eastern Europe and Russia.[115] Not withstanding the threats posed by botnets, the example of the Sumitomo attack shows how criminal elements are also utilising the physical element that that they know and understand and adapting it to attack using keyloggers against computer systems.

## 2.5 Summary

If we were to return to the example of Sumitomo, despite the lack of concrete information widely available, the alleged activity brings some excellent examples of the threat posed to organisations. The hardware keyloggers rumoured to have been employed to harvest the login credentials highlight that it is not only anomaly-oriented detection that is required to protect against attack, but that authorised access to a system can present the opportunity to undertake nefarious activity. This also highlights that no matter what technical controls are implemented, if they can be bypassed outside the scope of the original control then the full risk needs to be understood.

The fact that cleaners were able to access sensitive financial systems shows that the least important employees in the eyes of an organisation can have the greatest potential for unsupervised access, and only 55% of respondents to the dti survey[116] stated that conducted background checks on staff and/or potential staff.

Another example of the threats posed is provided within the dti report[117], where an employee of a firm used his laptop at home. When his system was connected to the corporate network after developing problems, it infected all their systems taking three days to disinfect all of the systems. To reiterate that point, one person caused major disruption to his organisation just by becoming victim to a malicious program! Also bear in mind that a lack of patching against a known vulnerability stopped the UK Coastguard from using their computerised systems throughout the country. All the facts point to organisations not being aware of the threats, the increase in vulnerabilities that require a person to assist with their exploitation is of concern with the vast majority of attacks being internal but no real changes are made to systems infrastructure to counter this threat. The reliance on an outdated view of the network perimeter is allowing companies to assume that their systems are safe behind the perimeter defences when criminal elements are actively attempting to subvert internal staff to gain access to their internal systems using phishing techniques. Companies cannot afford to assume that their internal systems will not become a staging point for attacks.

# 3 Discussion on the current state of enterprise security

Looking at the threats discussed above, there are a myriad of threats to protect against. As previously discussed, the very meaning of security is to provide protection from those threats. This chapter will discuss how enterprises protect against those threats.

All of the threats highlighted within the previous chapter have human interaction of some extent, whether it be an employee leaving their laptop in a taxi, becoming infected whilst browsing the internet or viewing an email, attempting fraud against a system or even failing to configure a system in a secure manner. So how do organisations protect themselves against these threats?

Given that just over 40% of respondents to the Deloitte security survey felt that security was still largely an IT function[118], one would assume that security is now perceived as a business function and attempt to protect against all threats, and not just the technological ones. From the responses within the same survey, this would not appear to be the case; with 74% of those organisations who had a Chief Information Security Officer (CISO) making that role report into the 'C' suite, only 48% of respondents felt security is considered a critical area of the business, and just over 50% of financial services respondents to the CSI/FBI survey felt that Sarbanes-Oxley had changed the focus from technology to corporate governance[119]. This would appear to be corroborated by the responses to the dti survey which showed that more UK businesses changed the configuration of their existing systems and/or deployed security technology than changed their policies and procedures or provided staff training after a major security incident[120]. This was despite 50% of all major security incidents being attributed to viral infections within the same survey[121]. This response is of

concern given the evidence provided in the previous chapter that signature-based technologies are being circumvented by the techniques employed by cyber criminals who are targeting the end user to facilitate exploitation of vulnerabilities.

In an interview (The full transcript of which is in Appendix III) with Peter Wood, Partner and Chief of Operations of First Base Technologies, the danger of this lack business visibility is shown *'where there is someone with a CISO-like role (albeit usually lower down the hierarchy than C-suite in our client base) then they are too often IT Security rather than Information Security…. This must change if real security is going to emerge as part of "business as usual". Most firms just don't understand this.'*

This use of technology to protect against the threats to an organisation would appear to be flawed, given that only 41% of companies felt either very confident or extremely confident about their protection against internal attacks[122]; with this figure rising to 74% in relation to protection against external threats. With over 87% of the same respondents[123] having deployed anti-virus, firewalls, VPNs, and spam filtering, these figures are understandable. However, given that the vast majority of incidents are internal, irrespective of the survey conducted, this would appear to show that organisations are reliant on technologies which provide protection against an external threat even though they are aware of the lack of protection against the statistically greater threat. (One of the technologies that could provide some indication of internal threats across the network environment, namely Intrusion Detection/Prevention Systems (IDS/IPS), was mainly deployed at the gateway between the internet and internal network by those organisations who implemented it[123], with 57% of organisations not having deployed the technology at all).

Peter Wood states that this concentration on technological security causes issues in instances of where *'the focus is strongly on IT security and specific controls therein. This makes security part of the IT function, which in turn is still seen as an overhead.'*

With the lack of faith in the ability of technology to fully protect against the internal threat, the alternative would appear to attempt to influence the behaviour of staff by other means. There also appears to be a lack of continuity relating to the methods adopted by organisations to tackle the threats related to people, with no methods employed by respondents to the 2006 dti survey reaching more than a 44% adoption rate[124]. The most commonly adopted methods to make staff aware of their obligations with regards to security were either during induction or via the staff handbook, with provision of training and/or presentations coming third. The first two methods would be seen as a 'one time' effort at best. This is also evident when looking at the Audit Commission report[125] which shows that majority of respondents felt that abuse of ICT systems was due to a failure to communicate the personal responsibilities to staff. This was almost double that of those who felt that lack of security awareness, adequate strategy/policies or the monitoring of processes were responsible for such activity. Deloitte also feels that[126] *'organisations are more likely to find themselves vulnerable to threats if employees are not aware of:*

- *Relevant policies*
- *Their role in helping to protect the information of the organisation*
- *How to support the organisation's security policies in the course of their day-to-day efforts'*

This perception is reinforced by an example[127] given within the dti survey where a large bank had experienced incidents due to staff misuse of email and web access. The incidents fell during the following year after an

improvement of monitoring processes within the acceptable use policy, combined with ongoing education of staff about the policy.

The difference in responses to the mitigation of two distinct threats within the dti report[128] also provides interesting reading, with larger businesses more likely to use technical controls and/or policies to stop staff from using removable media, and other companies more likely to do nothing. When the controls surrounding Instant Messaging (IM) were surveyed, whilst there was a difference between the reliance on the acceptable use policy to control staff, there was no real difference in the ratio of companies (Regardless of size) who did nothing to control IM. Ambivalence to each threat was as apparent as a desire to use policy to control the behaviour of staff; interestingly the level of ambivalence only differed with regard to removable media with larger businesses more likely to take action.

Interestingly, very few companies either protected the confidential data or restricted the usage of removable media and IM respectively. Both measures would appear to have the potential to mitigate the threat sufficiently rather than a reliance on controls.

As only 41% of EMEA respondents to the Deloitte survey[129] felt that they had both the required skills and competencies to respond effectively and efficiently and 61% possessed a security strategy[130], this would reinforce the notion of a disjointed response from companies, focussing on the technological aspects without looking at the complete risks. This disjointed response is more evident given the fact that only 66% of organisations who adopted a strategy felt that the strategy was led and embraced by business managers[130]. The dti survey further states[131] that *'a security policy in isolation is of limited use. It is important to link the policy to underlying technical standards and procedures. Risk assessment is an effective way of doing this. Assessing the threats and vulnerabilities that the business*

*faces enables control to be targeted to mitigate the exposure. Without a risk-based approach, a company can waste time and effort controlling the wrong things.'*

With only 40% of all respondent organisations to the dti survey having implemented a security policy[132], the problem would appear to be a lack of corporate governance rather than failures in technology. It should be stated that 73% of the large businesses surveyed possessed a security policy, and this would be expected due to the increase in security incidents experienced by this grouping from the responses within the survey. This grouping also experienced the most impact from staff misuse of information systems and theft or fraud involving computers, with 65% and 44% of large businesses respectively having experienced incidents of this type. The dti survey further states that the adoption of a security policy is different dependant on the priority that an organisation places on security[133]; 55% of all companies that gave a high or very high priority had a security policy compared to only 13% of those companies that made security a low priority.

This lack of corporate governance is evident within the responses to the Deloitte survey[134], with the greatest priority being given to regulatory compliance within the security initiatives being undertaken by financial companies. This concentration on compliance does not address the organisational issues, indeed concerning oneself with mere compliance has the potential to lead to a reactive security culture. Peter Wood again feels that priority given to such compliance *'will reinforce senior executives' view of security as a "necessary evil", since most entrepreneurs object to external "interference". However, it is likely to embed security more deeply in standard business processes which must help. Clever security managers may take the opportunity to convince execs of the value of security in this context, but it will be dependent on the individuals concerned. Often security people are not wholly realistic about business practices or ordinary*

*staff's attitudes and motivators, so they must change their own attitudes in order to take advantage of this change in the corporate landscape.'*

Whilst it is felt that security functions are moving from technical into more strategic areas, the pitfalls of a failure to understand the risks are highlighted within the commentary[135] relating to the initiatives being undertaken by respondents to the Deloitte survey to protect against identity theft/account fraud and identity management; where it is stated that *'while individuals most certainly contribute to the increase in identity theft it is an organisation's information management and security policies that are largely to blame. Many of the high profile customer data breaches…are the result of a failure of business practices, not solely of technology'*. With only 44% of respondents to the dti survey undertaking risk assessments[136], this inaccurate assessment of the threats to organisations and the causes of incidents will serve to further undermine a true understanding of the real issues affecting organisations and allow a concentration on technological remedies when sociological ones are also required.

This lack of understanding of the threats and risks affecting the enterprise, in turn, affects the ability to measure the performance of organisations with regards to their ability to protect against these threats. With only 43% of respondents to the Deloitte survey stating that their security employees had the security of the organisation linked into their appraisal process[137], this would reinforce that perception. One of the major issues with regards to the measurement of the performance of security functions is that there is no baseline for comparison. With the sociological aspect of the threats evident throughout this document, an increase in detection of malware could be due to a targeted attack, failure to patch a vulnerability, deployment of a new signature to detect the threat, being targeted due to the industry sector that the organisation is working in, or being hosted by an ISP that has come under increasing attack.

The measurement of security is therefore an intangible commodity, reliant on many factors, and certainly not assisted by security vendors who concentrate on the amount of different threats that they can protect against using technological means which is evident in any vendor-published whitepaper. With the vast majority of responses to threats being shown to be technological, and all the major security surveys from the past year relating the security spend to the IT budget and 82% of respondents to the dti survey using a formal business case to determine the spending priorities for security[138], it is very likely that the benefits of adopting the technological measures will have to be shown to justify expenditure. This can, in turn, lead to a concentration on and measurement of the performance of the technology rather than the protection against the threats.

Looking at one of the more common security publications, SC Magazine, the *'ThreatStats'*[139] section shows a wide range of different statistics on the top viral detections, phishing attacks, zombie/botnet statistics, spyware detection and 'zero day' attacks but not one of these statistical analyses discusses what the root cause of these infections are. As has already been discussed, the reliance on technological measures does not give confidence in the ability to protect against the threats to the enterprise, but rather the security vendors influence the creation of an environment whereby organisations measure what they can, rather than what they must.

This simplistic measurement allows vendors the opportunity to show impressive statistics relating to the amount of threats that they can protect against, even though research[140] shows that often the groupings behind malware such as MyTob are releasing multiple variants per day. It could be argued that as most security vendors rely on the subscription-based business model whereby an annual fee is required to maintain protection against the threats, that this simplistic measurement within the enterprise

benefits the vendors at the cost of understanding the underlying risk, as previously discussed.

With just over 80% of dti respondents who stated they gave a very high priority to security not having any security staff with formal security qualifications[141], this lack of understanding of the underlying risk is to be expected; with the same survey showing that 75% of qualified security professionals were likely to conduct a risk assessment compared to the 44% average[142]. It is of note that organisations who gave a very high priority to security also spent the most on security, a figure that was matched by those organisations that had conducted a risk assessment[143]. Given the preceding statistics, it could be alluded that whilst the expenditure on security is the same, the effectiveness and efficiency of that spend would be expected to be greater for the organisations who had conducted a risk analysis.

The focus on the technological remedies necessitates that security initiatives vie for a share of the IT budget, as has already been confirmed throughout the security surveys conducted. This ensures that security initiatives will be seen as a cost, overhead or even a 'tax' as it were of conducting business. The downfall of this is shown when looking at the value that technology can provide. When looking at the dictionary definition of 'value'[144], amongst the terms of worth and equivalence is the term utility. This could lead to a definition that value is related to usefulness, and therein lies the main issue with technological security – it isn't perceived as useful due to being marketed as one-dimensional, in that it only protects against threats.

Other technologies are marketed as allowing businesses to do things better, stop doing things (ie save money) or do new things (ie make money.). These technologies are, in turn, seen as being more useful and

consequently have more value assigned to them. As long as security is seen as providing purely technological remedies, this will always be the case.

Whilst it is true that the purpose of security is to protect against threats through controls, an example of how a control can also be an enabler is given within the book *'Enterprise Security Architecture – A Business-Driven Approach'*[145]. An example[146] is given of a braking system within a car. This certainly stops the car but better brakes allow the car to be driven safely at faster speeds. This is an excellent analogy, and shows that an understanding of the purpose and the risk allows an appropriate control to be implemented to enable greater performance. To continue the analogy, a one-dimensional control could be illustrated as the seat belts in a car, whereby an improvement in the quality of the seat belt would not have the same enabling effect with regards to performance. Controls can be useful, but the perceptions must change.

## 3.1 Summary

Whilst the vast majority of organisations feel that they are giving priority to security, the evidence points toward a largely technological approach that provides protection against the perceived external threats but one in which the companies have no confidence with regards to the internal threats. This reliance on technological controls is also reinforced with all the major surveys on security produced within the past year relating spend on security to the IT budget. This perception of security being seen as a mainly technological function results in it being seen as an overhead rather than a benefit.

Although the security benefits of technological controls are without question, research points toward the need to provide an additional

sociological remedy to the threats posed, although there appears to be a reticence to moving towards this. This could be construed to be due to the controls being one-dimensional and providing no usefulness to the organisation. Without a change in the perception given towards controls, and boardroom support, it will be very hard to fully understand the benefits of these controls. The lack of importance given toward elevating the visibility of the security function to the boardroom, which in turn affects the facilitation of corporate governance, is of concern.

The measurement of the performance of security would also appear to be insufficient due to a lack of risk assessment relating to the vulnerability to the threats, and a reliance on using vendor-supplied performance metrics which have no relevance on the underlying causes of the incidents and merely serve to provide a justification to spend more on technological controls.

# 4 Improving the value perception to the enterprise

It can be seen from all of the discussions thus far, that security functions face a number of issues:

- *Perception*

  Security functions are perceived as providing one-dimensional controls, which mainly focus on technological methods. These controls are not seen as being useful to organisations in improving business performance, and are felt to be more appropriate to 'keeping the bad guys out'. The benefits resulting from the adoption of security controls need to be seen in terms other than that of a control function.

- *Understanding*

  Aside from the perception of security controls, businesses need to understand why they are being asked to adopt controls. This has the potential to affect the performance of the sociological controls required to fully mitigate against the threats encountered. In addition, businesses need to understand risks to their environment and communicate their drivers to allow an understanding between the boardroom and the security function. This would ensure that security will not be viewed as a purely technological function that, in turn, is part of the IT budget.

- *Structure*

Security functions need to adopt structures that can be reused and become proactive. Security strategies need to be seen to enable business by facilitating the adoption of new technologies and business processes and possess the ability to link upward to show a direct lineage from the business drivers.

- *Measurement*

  Security is an intangible commodity, and as such is difficult to measure. Measurement has to currently be provided to obtain funding and, as most of the controls are technological, a measurement on the performance of technology is usually undertaken. This results in an inaccurate picture of the ability of the organisation's security posture. With a resolution of the issues above, a more accurate measurement can be undertaken of the realisation of the benefits of security implementations and their resultant usefulness, and hence value, to the organisation.

The remainder of this chapter will discuss relevant research and various methodologies that can be employed to address the issues highlighted above. The order of the issues, as detailed above, is deliberate as it is felt that each is inextricably linked into the preceding and/or following issue(s).

## 4.1 Improving perception through the illustration of benefits

Given that the majority of responses to security issues have been shown to be technological, it is deemed appropriate to show the benefits of the adoption of these technological measures to the enterprise. This concentration on the technological issues is deliberate and the sociological issues will be addressed later in the following sections of this chapter.

The business value model[147], conducted after research by Melville et al, is seen to draw from various research to propose a model concentrated on a resource-based view (RBV) of an organisation. The model focuses on the resources available to the organisation rather than the market in which the organisation operates. The resources included are not only the physical and financial assets, but also includes the skills and experience of the employees. This view of the organisation theorises that if a resource is rare and/or difficult to imitate then the resource can provide an advantage to the organisation. This advantage can also be termed a value to the organisation, and its worth is dependant on the availability of this resource to other organisations.

The premise of this research is that IT resources (Both technological and human) act in conjunction with other complementary organisation resources (eg Working practices and/or organisational culture) to provide the basis of the processes of the organisation which would be expected to engender increased organisational performance.

The research found[148] *"that IT is valuable, but the extent and dimensions are dependent upon internal and external factors, including complementary organizational [sic] resources of the firm and its trading partners, as well as the competitive and macro environment."*

Building on this research, which is accepted in its entirety, it would appear to be a reasonable assumption that all technological implementations can provide value. Based on this research the diagram shown overleaf, which is based on the business value model created by Melville et al, shows the factors that can influence the

success of a technological security implementation. These factors have been drawn from the all previous discussions within this document.

The external factors deemed to influence the generation of business value by Melville et al are:

- *Macro environment – Country characteristics*

  The country in which the organisation is operating will have it own legislation that will affect the operation of the business. Examples of this are the Sarbanes-Oxley and Patriot[149] Acts within the United States and DPA 1998 and CMA 1990 within the UK. In addition, the threats from the legislation enforced to protect against cybercriminals attacking the organisation and the adoption of high-speed internet connections amongst the population of a country can affect the threats to an organisation.

- *Competitive Environment – Industry characteristics*

  The industry in which the organisation operates will usually be subject to regulation unique to that industry. Examples of this are the HPIAA[149] Act within the US and Financial Standards Agency (FSA)[150] within the UK. The implementation of high-cost initiatives by organisations within the industry can also present pressures on competitors, with the recent implementation of two-factor authentication by several retail banks within the UK being a prime example.

Both of the above characteristics would be deemed to be mainly tangible in nature due to the legislation/regulation being clearly defined.

- *Macro Environment – Trading partner resources and business processes*

  As has been previously discussed, many companies do not restrict the systems that trading partner employees can access, preferring to rely on contractual agreements. The lack of full understanding and control of the quality of the security of a trading partner must make this an intangible characteristic and considered as being a potential external threat. This external threat could be deemed to be even more dangerous that a targeted hacking attempt due to the lack of network and/or systems controls.

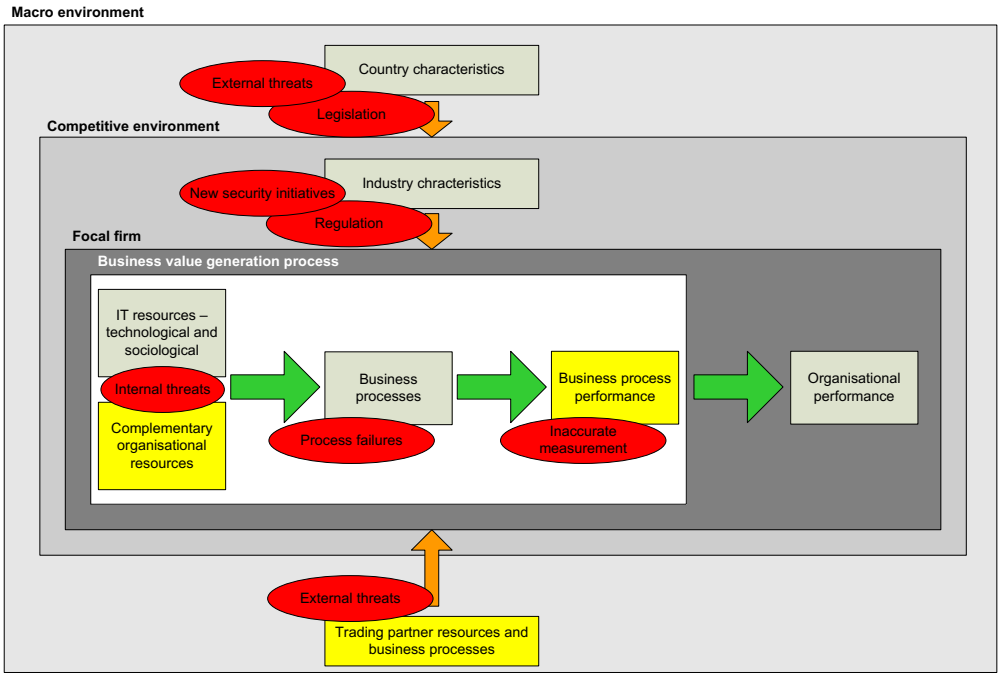



**Figure 4-1 Business resource model with threats**

Within the organisation, the following resources are deemed to be important to generate business value and hence improve organisational performance:

- *IT resources – technological and sociological*

  The IT resources available to an organisation, whether they be a technological system or human being involved in the operation or support of IT would be deemed as being tangible assets. As previously discussed, however, the internal threats to and by technology and people are considerable.

- *Complementary organisational resources*

  The working practices and culture of an organisation are felt to be important factors in the success of technological implementations. These resources are often hard to define and are more due to behavioural characteristics, as such they should be considered an intangible commodity. As behavioural characteristics have already been shown to affect the facilitation of internal threats, this behaviour needs to be controlled.

- *Business processes*

  The business processes adopted within an organisation are generally defined within an organisation, as their value is understood by organisations. However, without a full understanding of the internal threats, especially the behavioural characteristics of employees processes can fail to adequately

control these behaviours. This leads to issues with regards to corporate governance.

- *Business process performance*

  In the event of a failure to ensure that the business processes are adequately defined to ensure corporate governance, the measurement of the performance of business processes would not be deemed to give a true picture. Certainly, with regards to performance from a security perspective we have already discussed how organisations do not fully comprehend the threats to their organisation and undertake simplistic measurement of the technological controls. This leads to inaccurate measurement and an intangible commodity.

All of these factors influence the organisational performance, which itself is often measured in financial terms, whether it be to maximise profit or minimise expenditure.

From this model, it can be shown that whilst technology can create value, it cannot achieve this without understanding the external threats, relevant legislation/regulation obligations, internal threats, interaction with corporate culture/working practices, potential for process failures and the need for accurate process performance measurement. Research conducted for the Harvard Business Review showed[151] that IT investment did not improve productivity alone; it was the application of technological measures by organisations that mattered most.

The three most critical factors that were deemed to result in the largest gain for organisations who invested in technological solutions were:

- *Target the productivity levers that matter*

  Concentrate the implementation of technological solutions to the influencing factors that matters most to the organisation.

- *Get the sequencing and timing right*

  Ensure that the deployment of technical systems is scheduled to ensure the availability of relevant business processes and/or technical systems.

- *Pursue managerial and technological innovations in tandem*

  The study states that *'History shows that technological innovations are typically of little use until managerial practices adapt to them'*. Business changes are required to effect the maximum benefit from technological solutions.

Other research has been undertaken into providing the generic benefits that technological implementations can provide to organisations by augmenting Mintzbergs[152] *Structure in Fives* view of an organisation. Mintzberg felt that there were five elements of an organisation, which after research conducted by Farbey et al[153], was defined into the following areas:

- *Strategic*
- *Management*
- *Operational*
- *Functional*
- *Support*

Whilst a full list of the generic benefits of IT after further research from Ward et al, is available[154], some examples of the benefits that IT can provide will be discussed here.

Examples of strategic benefits from IT are in the realms of eCommerce, where a service can be provided by small-medium enterprise that would normally be able to reach its customer base due to geographical constraints.

The benefits of IT for the managerial element of an organisation can be exemplified in the provision of agility. The following are deemed to be the capabilities required to enhance business agility[155]:

- *Intelligence* – The ability to respond to changes in customer need or market conditions
- *Competences* – The speed in which new process, technological and managerial skills can be adopted
- *Collaboration* – Effectiveness of interaction between different business departments, and/or the ability to reassign resources between projects with ease
- *Culture* – Empowering independent decision making amongst employees
- *IS* – Ability to rapidly introduce new Information Systems (IS) through the support of the IT infrastructure.

Operational benefits from IT can include increased efficiency and timely access to data, and reduction in costs and human resources. This can also allow internet access to data for customers.

The benefits of IT for functional/support roles can include remote support, self-support systems and the enforcement of regulatory and/or legislative requirements.

From their research, Farbey et al identified[156] that many of the IT implementations also achieved unplanned or emergent benefits in addition to the original benefits planned from the implementation. In many cases, these emergent benefits were deemed to have arisen from the achievement of a planned benefit. Interestingly, these benefits were also deemed to be associated with the perception of the systems by individuals involved with the system and their satisfaction with it and were of a largely intangible nature[157].

Ward et al, balance the benefits that can be derived from the engagement of technological solutions with a discussion[158] relating to the negative effects or 'Disbenefits' that IT implementations can provide. Increases in efficiency can lead to reductions in human resources, implementation of security solutions can stop activity that has normally been carried out, mobile email devices (Such as Blackberries) can encroach into the home life and affect the life/work balance.

The DeLone and McLean Information Systems (IS) success model[159], shown overleaf, is a widely used framework for measuring the success of information systems.

Within this framework, the net benefits after consideration of the benefits and disbenefits of a system are deemed to directly feed into the satisfaction of the end user and their intention to use the system.

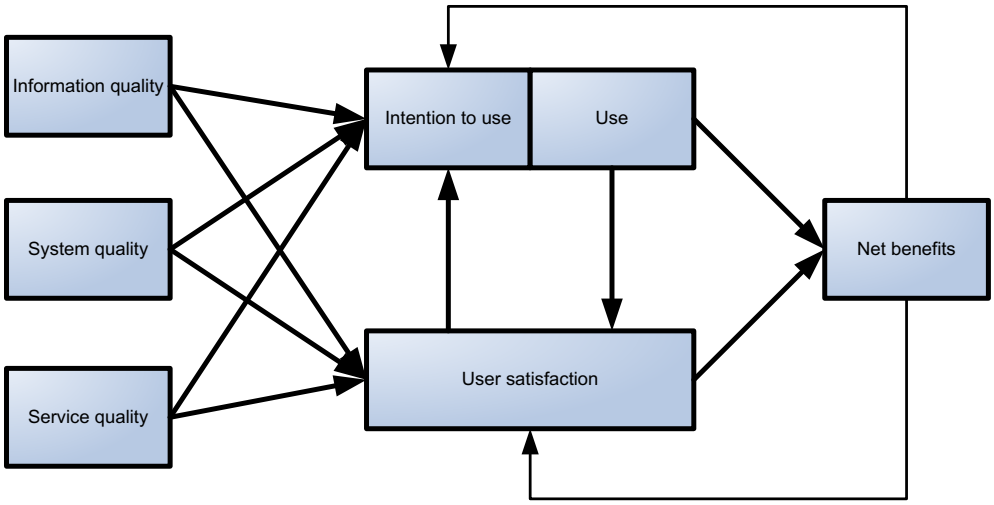



**Figure 4-2 DeLone and McLean IS success model**

As can be seen from the figure above, the actual experience in using the system and the user satisfaction feed into the net benefits. A system that is not used due to these perception issues will undoubtedly fail to be perceived as being valuable. The benefits previously discussed should be considered in the light of who the benefit is to be directed to.

Further to the issues previously raised, research by the Cranfield School of Management[160] found that whilst 55% of organisations felt that an appraisal of their IT investments was seen as being important by business managers, 78% didn't have an effective investment appraisal process, 70% didn't adequately involve business managers and 90% of appraisal processes didn't consider the implications of business changes as a result of the investment. In addition, 75% of organisations felt that people making the investment decisions didn't understand the business cases and 73% of projects didn't deliver the benefits that justified the initial investment.

The above research shows that there is a lack of interaction between IT staff and business managers, which is contrary to the conditions for productive IT investment previously discussed in this section. Given that 82% of respondents to the dti security survey stated that they determined expenditure on security project by means of business cases; the above results would also appear to indicate that if normal IT investments are failing in the manner described, then technological security measures would not be expected to be performing differently. This is reinforced by the results of the Deloitte survey in which only 47% of respondents felt that their board understood the major security investments from a risk and return viewpoint[161].

In the event of a lack of understanding of the business cases and involvement with business managers, it is very likely that the financial aspects of the investment proposal would be the basis for a decision. With the lack of consideration for the required business changes that have already been identified as being important for the successful implementation of technological solutions, those technology-based security projects that are approved will either fail to realise the benefits or require additional capital expenditure.

This need for the importance of understanding the need to consider business changes is highlighted in a report by the iSociety[162] which stated that *'New technology is not transformational on it own … appropriate use requires considerable complementary investment in people, process, culture and support … some or all of these things are usually missing'*.

Another model that can illustrate steps involved in creating value from IS/IT investments is provided by research from Soh and Markus[163], shown overleaf, whereby three distinct processes are required to be

undertaken.

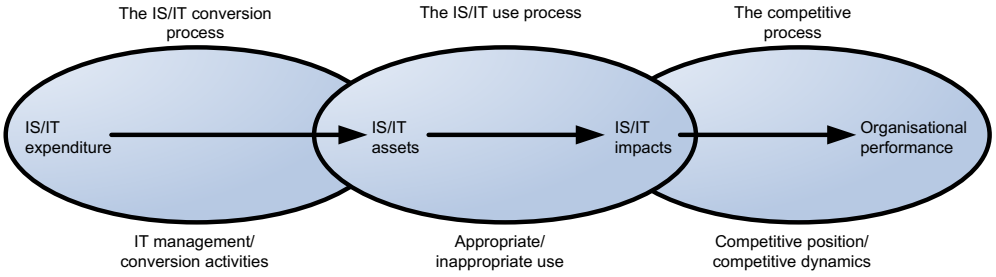



**Figure 4-3 Soh and Markus model**

The IS/IT systems purchased are converted into assets for use by the organisation; these assets must then provide an organisational impact. The final stage is the effective utilisation of the assets to improve organisational performance.

The provision of impact to organisations from IS/IT is stated to occur *'when people and organizational units use IT assets (technology and skills) appropriately, a process affected by organizational structures, processes and culture'*[164]. This reinforces the notion from DeLone and McLean that successful technological projects are reliant on the understanding of the perspective of those people that will be affected by the technology, by using the technology or otherwise. The people, often termed stakeholders will react differently based on their perception of the benefit to them. In the event of people having to change their working practices/processes or using the system, then their perspective should be understood to facilitate a success implementation.

Given all of the issues relating to the realisation of benefits relating to technological investments, it is recommended that Benefits Management methodology by Ward et al[165] be followed. The benefits management methodology allows organisations to make progress as shown below.

- Focus on the delivery of benefits rather than technology
- Focus on the tracking of the delivery of benefits during projects
- Providing business cases linked to organisational strategy and/or objectives
- Understanding the need to undertake business changes through change management to complement the implementation of technology
- Involving business managers in all stages of the process to gain commitment through collaboration
- Defining the benefits required from a system rather than picking from the features of technological solutions
- Involving stakeholders in the process
- Ensuring staff understand how to exploit the technological systems to realise the intended benefits
- Undertake post-implementation benefits review

This methodology is based on the 'real world' experience of the authors and is not a theoretical methodology. It is of note that the authors make the distinction between Information Systems and Information Technology in definition that Information systems are *'the means by which people and organisations, utilising technology, gather, process, store, use and disseminate information'* and Information Technology supports Information Systems. It is intended that sufficient detail shall be provided within this document to provide an overview of the process. For further information, it is recommended that the referenced text be consulted.

The methodology makes the assumption that organisations possess a business, IS and IT strategy as defined below:

- *Business strategy* – Defines objectives and direction *(ie 'Where is the business going and why?')*
- *IS strategy* – Based on the business strategy, demand oriented and applications focused *(ie 'What business support is required?')*
- *IT strategy* – Based on the activities of the organisation, supply oriented and technology focussed. *(ie 'How can it be delivered?')*

The authors state that there should be a separate IS strategy to ensure that the delivery of applications focus on the meeting business needs rather than concentrating on the technology required to deliver them.

The benefits management process is based on the following processes:

- Establish the external and internal business drivers

  These are defined[166] as being *'views held by senior managers as to what is important to the business – in a given timescale – such that they feel changes must occur. Drivers for change can be both external and internal but are specific to the context in which the organisation* operates'. As such, it is envisaged that these drivers will be provided by the senior managerial functions within the organisation and are therefore out of the scope of this document. For further information on how business drivers are determined, it is recommended that the referenced book be referred to.

- Establish the investment objectives

These are the *'organisational targets for achievement agree for the investment in relation to the drivers. As a set they are essentially a description of what the situation should be on completion of the* investment'[167]. It is recommended that the list of objectives be as brief as possible.

- Link the investment objectives to the business drivers

The purpose of this stage is to ensure that the intended objectives can be shown to link with one or more business drivers. This is designed to ensure that the projective objectives remain linked to the desired business priorities rather than the features of the software/system being implemented. The following diagram provides an example of how to record this linkage:

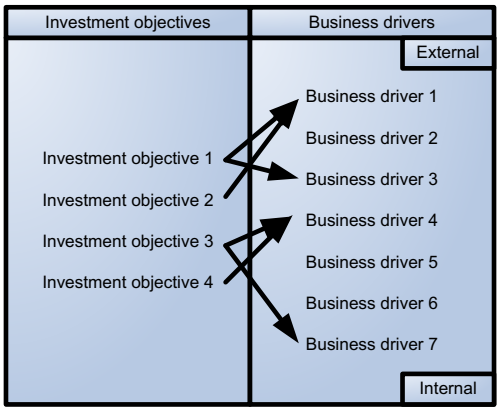



**Figure 4-4 Linking objective to business drivers**

As can be seen, there is no requirement to link objectives to all business drivers. The completion of this framework should be from right to left, as is the standard with all frameworks used within this methodology.

- Identify all potential benefits that could be realised by achieving the investment objectives by talking to stakeholders
- Understand what combination of IS/IT functionality and business changes could cause the benefits to be realised by talking to stakeholders
- Establish ownership of the benefits and determine if the benefits can be measured to prove their realisation by talking to stakeholders
- Identify any organisational issues or implications for particular groups of people (Stakeholders) who:
    - will benefit from the investment
    - is directly involved in making changes, or
    - is affected by the changes need to realize the benefits

  and could hinder or even cause the project to fail

  These stakeholders can be categorised using the summary stakeholder assessment tool below:

| Benefits received | Changes required: LOW | Changes required: HIGH |
|---|---|---|
| HIGH | NET BENEFITS<br><br>Should champion the project – but must be aware of implications for others and user their influence<br><br>*Collaborators* | BENEFITS BUT ….<br><br>Will be positive about the benefits but concerned over changes needed – ensure sufficient enabling changes are identified to offset any resistance<br><br>*Compromisers* |
| LOW | FEW BENEFITS BUT …<br><br>Must be kept supportive by removing any inertia/apathy that may influence others<br><br>*Accommodators* | NET DISBENEFITS<br><br>Likely to resist changes – must ensure all aspects of resistance are dealt with by enabling projects<br><br>*Resistors* |

**Table 4-1 Stakeholder assessment tool[168]**

- Produce an outline business case to decide whether to proceed further or stop the investment now. The benefits should be classified using the following framework used for analysing the benefits:

| Degree of explicitness | Do new things | Do things better | Stop doing things |
|---|---|---|---|
| Financial | | | |
| Quantifiable | | | |
| Measurable | | | |
| Observable | | | |

**Table 4-2 Framework for measuring benefits[169]**

It is deemed that the value of benefits will either be classified as where[170]:

- *'the organisation, its staff or trading partners can do new things or do things in new ways, that prior to this investment were not possible'*
- *'the organisation can improve the performance of things it must continue to do'* – it can do things better
- *'the organisation can stop doing thing that are no longer needed'*

In addition, the performance of benefits is deemed to be able to be classified in one of the following ways:

- *Financial* – in the event that a benefit is quantifiable, a financial value can be calculated

- *Quantifiable* – Where *'sufficient evidence exists to forecast how much improvement/benefit should result from the changes'*
- *Measurable* – Measurement is possible, but estimation of the improvement in performance is not possible
- *Observable* – Experience of judgement could be employed to determine the extent to which the benefit has been realised

- If the outline business case provides sufficient evidence of merit, then provide a full description of each of the benefits and changes, with clearly defined and agreed people with responsibility for delivery
- Agree ownership of the planned changes and actions to counter all stakeholder issues that may impact the implementation of the business, enabling and IS/IT changes
- Create the benefits dependency network

The benefits dependency network is one of the key frameworks within the benefits management methodology and consists of the following components:

- *Investment objectives*

As previously discussed

- *Business benefits*

A business benefit is defined as *'an advantage on behalf of a particular stakeholder or group of stakeholders'*[171]. The benefits specified should be

descriptive, for example a typical benefit given could be one of 'improved decision making'. For the purposes of this framework, the group/individual that would benefit and how they would benefit should be entered.

- *Business changes*

  These are *'the new ways of working that are required to ensure that the desired benefits are realised'*[172]. Business changes are not normally able to be undertaken until the new system is available and the relevant enabling changes have been made.

- *Enabling changes*

  Defined as the *'change that are prerequisites for achieving the business changes or that are essential to bring the system into effective operation within the organisation'*[173]. It is of note that neither the business nor enabling changes are required to link to an IS/IT change as it is feasible that a change must be affected separate from the technological implementation. In addition, due these changes potentially being required to amending working practices or some other change in relation to the adoption of the new system, they often can or must be undertaken prior to the introduction of the new system.

- *IS/IT enablers*

These are *'the information systems and technology required to support the realisation of identified benefits and to allow the necessary changes to be undertaken.'* [174] These enablers could either be new systems and technologies or existing ones. The completion of the benefits dependency network from right to left allows a more accurate determination to be made as to whether the technological changes are required, or if the benefits could be realised by making organisational changes. These enablers can also show dependencies on each other.

An example of the information and structure of a benefits dependency network is shown below:

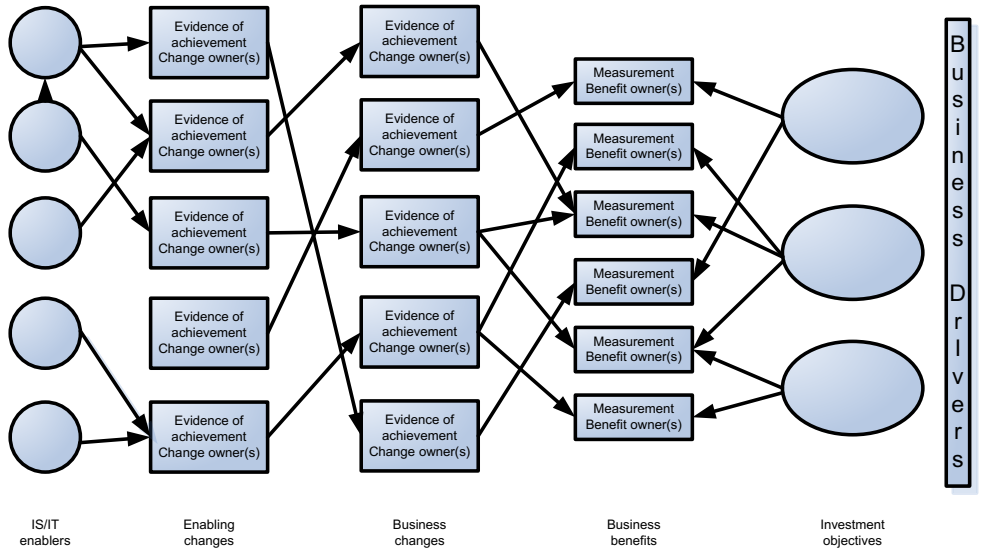



**Figure 4-5 Benefits dependency network**

One of the key advantages to this approach is that the benefits gained by the adoption of security controls within a project are evident. Also the methodology ensures that even with the adoption of a purely technological security control, that the people who are affected by the

control are consulted, additional benefits can be realised and shown and changes are made to business processes to effect maximum benefit from the investment in the technology. This has the very real potential to address the perception issues relating to security controls.

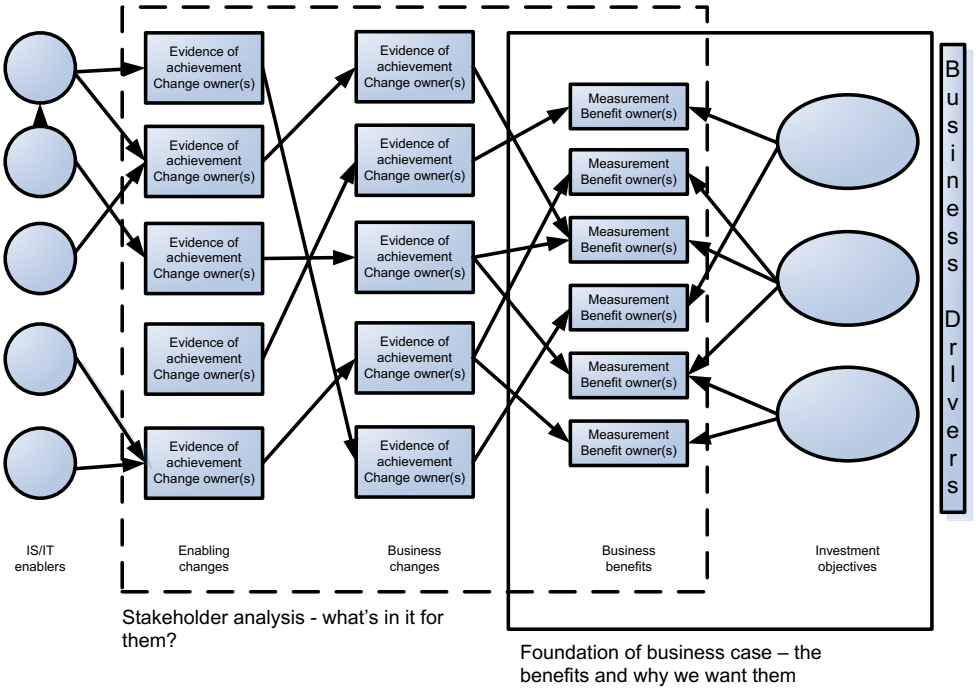



**Figure 4-6 Benefits dependency network showing stakeholder and business case areas**

The benefits dependency network allows a reference point to start from to conduct the stakeholder analysis by looking at the business benefits, business changes and enabling changes to determine who will be affected by these changes and how the illustration of benefits in this can improve the perception of the implementation. The foundation of the business case can be found when concentrating on the business benefits and the investment objectives.

The visible reference of the benefits dependency, linkage into the business drivers and the ability to show the value and performance of the benefits is of great use in the facilitation of understanding from the

people making the investment appraisals, and has the real potential to change the view of technological security investments from being purely one-dimensional controls to having further usefulness and value to the organisation.

## 4.2 Improving understanding through alternate learning techniques and risk assessment

The employment of workshops, as recommended by the benefits management process will greatly increase not only the understanding of people who will be affected by security implementation, but also the engagement of the business managers who will be affected. The recommended approach of assigning a senior business manager with not only the required influence within the organisation, but also the drive and availability to lead the project, as the project sponsor will assist with the management support for security implementations. It has already been show that the process has the very real potential to not only involve the business within security projects, but also provide a non-technical person with the facility to understand the interaction between the security function and the achievement of benefits.

The involvement of the business drivers in both the benefits management and SABSA®[175] methodology, which will be discussed in more detail in the following section, ensures that security professionals engage with the business and are better placed to present solutions that not only mitigate against risks to the enterprise, but also allow the enterprise to continue to function in a manner compatible with their desired strategy.

Once the perception of the security function within the enterprise has been changed, the next recommended step is to facilitate an enabled

learning environment for the end users and ensure the understanding of the senior management of the organisation with regard to the risks present within their organisation.

We have already discussed in previous chapters that the need for sociological controls is increasing. The end user is more important in ever in the security of an organisation. Whilst the amount of organisations conducting security awareness programmes is on the increase, the manner in which they undertake this awareness training is of concern. It has already been shown that research indicates that people conduct activity at work that they would not conduct at home due to a feeling that their employer has better security controls or that there is support available if something goes wrong. The concentration on the application of technological controls perpetuates the notion that security is not the concern of the end user, and is the responsibility of the security functions within the organisation. This notion is based on the premise of pedagogy[176], a learning style that is directed towards children.

The learning in this methodology is concentrated on the direction of learning originating from the teacher (In this case the policies of the organisation or presentations from the security function), with minimal control available to or understanding required of the person learning the subject material. Pedagogy is dependant on the teaching ability of the teacher, and merely imparts information to the student. The pedagogic style of learning also encourages convergent thinking, which although it might be felt that this is desired is exactly the opposite of what is required to have the skills to adapt to the dynamic threats presenting themselves today.

It is felt that the andragogy[177] style of teaching is more suited to the education of end users in the subject of information security. This style, which is derived from the educational theory of Plato and deemed to be more suitable for adult learning, concentrates on the understanding of the student as to why he/she is undertaking the learning. This context would ensure that people wish to learn what is being taught, and therefore a state of 'active learning' can be achieved, encouraging divergent thinking an placing as much emphasis on the student as the teacher to facilitate continued learning. The style also encourages an assimilation of life experience with learning, and places the responsibility for learning on the student.

Malcolm Knowles, a leading proponent of the andragogic teaching style states that *'Andragogy assumes that the point at which an individual achieves a self-concept of essential self-direction is the point at which he becomes adult. A very critical thing happens when this occurs: the individual develops a deep psychological need to be perceived by others as being self-directing. Thus, when he finds himself in a situation in which he is not allowed to be self-directing, he experiences a tension between that situation and his self concept. His reaction is bound to be tainted with resentment and resistance.'*[178]

Whilst there is some debate[179] over the importance given to the andragogic theorem as defined by Knowles, this mainly concentrates on the inefficiency of his emphasis on the student to learn from peers. It is of note that the critiques of the theorem[180] still recognise that it has value in the addressing of the resentment and resistance to learning by traditional pedagogic techniques.

It is recommended therefore that this style be followed when undertaking security awareness training, concentrating on the subject

of home-based security awareness. This is due to the need to assimilate learning with life experience, and place the responsibility for understanding information security-related issues onto the end user. This approach will also ensure that the end users feel that the awareness programme is of relevance and use to them. The understanding from an effective awareness programme that engages the interest of the end user would be expected to avoid the feeling of resentment and resistance alluded to by Knowles.

In order to address the issues relating to the understanding of the information security risks inherent within the enterprise, security functions need to tackle the lack of risk assessment within organisations. The lack of information security risk assessment within organisations is disappointing low given the results from the dti security survey. The lack of this risk assessment could be attributed to 79% of all respondent organisations to the dti survey feeling confident about having capturing all breaches of notes during the past year[181]. This trend is followed by the 84% of respondents to the Deloitte survey who stated that they had taken the necessary steps to protect their IT assets[182], this is even more interesting given that only 52% respondents to the same survey felt that their level of risk was effective and efficient.

As only 44% respondent organisations to the dti survey had conducted risk assessments during the same period it is unlikely that these figures are based on a true understanding of the inherent risks and could therefore be considered less reliable. It is even less likely that organisations will be fully aware of security breaches given that research within the Audit Commission report showed only 32% of respondents knew where to find documented procedures for reporting a security incident[183].

Given that organisations, by their very nature, undertake corporate risk assessments on a regular basis; this lack of information risk assessment is of concern and would indicate a lack of willingness from the enterprise to assimilate information security risk into the corporate governance framework.

With over 60% of respondents to the Deloitte survey failing to experience any convergence between the physical and logical security functions[184], increased interaction could assist in the perception of the risks posed to the enterprise. It is also very likely that whilst logical security functions are still branded as being IT Security, they will continue to be seen as being technologically-focussed. Another issue with regards to the risk perception of logical security threats is provided within the Deloitte survey[185], with only 12% of respondent organisations having an individual with responsibility for both information and technical security. Of the remaining organisations, only 25% have a reporting structure that's allows the separate individuals with responsibility for information and technical security to report to the same senior manager. This fact further serves to cloud the risk perception, and further undermines the ability of the enterprise to undertake effective corporate governance.

It is therefore recommended that security functions consider simple remedies to promote the understanding of their role within the organisation. Collaboration with physical security functions can assist in this manner, as can the simple rebranding of security functions (Changing the name of the function from IT Security to Enterprise/Corporate Security for example). Risk methodologies employed also need to take account of new threats to the enterprise and include the assessment of authentication risks in conjunction with

the standard Confidentiality, Integrity and Availability risks usually assessed.

With more efficient, effective and relevant risk assessment techniques, talking the same risk language of the business and understanding what is important to the business, this can have an impact on the ability of senior management to understand the risks to their organisation and therefore understand the need for improved corporate governance. This will, in turn, result in better 'buy in' from senior management for improved corporate security initiatives. However, this will become harder to achieve unless the benefits that can be realised from existing security expenditure and involvement can be seen; making the benefits management techniques previously described more important.

## 4.3 Improving the performance of security by creating security architecture

With an improved perception and corporate governance profile related to security functions and their activities, the disjointed reaction to security challenges can now be addressed. Technical architecture has been employed within the enterprise for some time now but, as with it's physical equivalent, without a business driver the most beautiful and complex architecture can fail to achieve fruition. A classic illustration of this is Gaudi's cathedral[186] in Barcelona, a feat of architectural beauty and still unfinished over a century after the project initiation whereby the office blocks within any major city can typically be erected and made operational within a matter of months. In the same vein, it has to be understood that after the completion of the architectural implementation regular maintenance must be conducted

to ensure that the design still provides the function for which it was originally designed for.

Security architecture is no different, and requires an illustration of the benefit that it will bring to an organisation's business drivers to ensure successful adoption. The Sherwood Applied Business Security Architecture (SABSA®) methodology is considered to address the issues described within this document and can create an environment to enable the agility required to 'Do New Things' as defined by the benefits management methodology. Both are deemed complimentary to each other, as the realisation of benefits is covered in greater detail by the benefits management methodology whilst both provide strong links into business drivers.

The SABSA® methodology is derived from the enterprise systems architecture framework created by Zachman[187], with the equivalent stages between shown below:

| Zachman's views | SABSA architectural equivalent |
|---|---|
| The Business View | Contextual Security Architecture |
| The Architect's View | Conceptual Security Architecture |
| The Designer's View | Logical Security Architecture |
| The Builder's View | Physical Security Architecture |
| The Tradesman's View | Component Security Architecture |
| The Facilities Manager's View | Operational Security Architecture |

**Table 4-3 Correlation between Zachman and SABSA® methodologies[188]**

The implementation of these architectural components within the SABSA® methodology is shown overleaf:

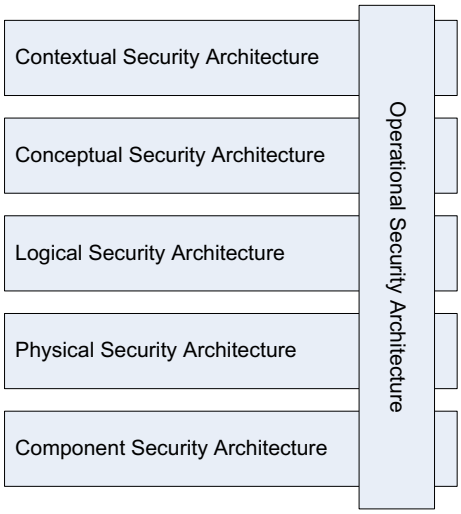



**Figure 4-7 SABSA® Architecural layers**[189]

The operational security architecture is placed across all of the other architectures due to operational security being implemented at all layers of the architectural framework.

The SABSA® methodology ensures that each layer has a link into the pervious and/or following layers, as shown below:

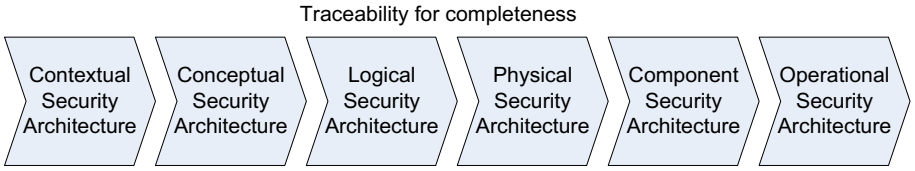



**Figure 4-8 Traceability through architectural layers for completeness**[190]

This linkage ensures that all stages of the framework are completed, providing a consistent experience throughout the architectural documentation. The framework also provides a means to link each stage of the framework to the business drivers and priorities, as illustrated overleaf:

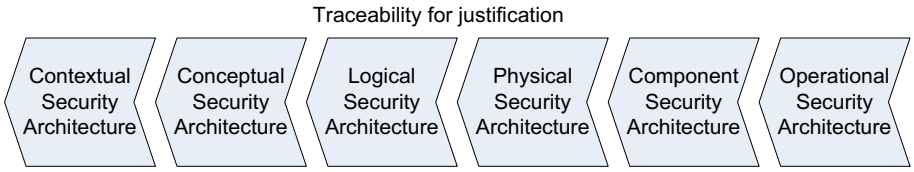



**Figure 4-9 Traceability through architectural layers for justification[191]**

In order to better understand the implementation of the SABSA® methodology, and the interdependencies previously mentioned, the SABSA® matrix is used

| | Assets (What?) | Motivations (Why?) | Process (How?) | People (Who?) | Location (Where?) | Time (When?) |
|---|---|---|---|---|---|---|
| Contextual | The business | Business risk model | Business process model | Business organisations and relationships | Business geography | Business time dependencies |
| Conceptual | Business attributes profile | Control objectives | Security strategies and architectural layering | Security entity model and trust framework | Security domain model | Security-related lifetimes and deadlines |
| Logical | Business information model | Security policies | Security services | Entity schema and privilege profiles | Security domain definitions and associations | Security processing cycle |
| Physical | Business data model | Security rules, practices and procedures | Security mechanisms | Users, applications, and the user interface | Platform and network infrastructure | Control structure execution |
| Component | Detailed data structures | Security standards | Security products and tools | Identities, functions, actions and ACLs | Processes, modes, addresses and protocols | Security step timing and sequencing |
| Operational | Assurance of operational continuity | Operational risk management | Security service management and support | Application and user management support | Security of sites, networks and platforms | Security operations schedule |

**Table 4-4 SABSA® matrix[192]**

As can be seen from the matrix above, each layer find it's purpose (Motivation) from the layer above, and this eventually leads to the business risk model.

The sections for each layer are defined from the following questions:

- What *assets* are you trying to protect at this layer?
- What is your *motivation* for wanting to apply security at this layer?
- What *process* are you going to follow to achieve security at this layer?
- What *people* and/or human resources is affect by security at this layer?
- Where is the *location* of where you are going to apply security at this layer?
- At what *time* that you are going apply your security?

An interesting approach undertaken by this methodology is to include areas that would often be considered operational in nature such as capacity planning and network design. Given the threat posed by Denial of Service (DoS) conditions to the enterprise at present and threats posed by 'fuzzing' techniques previously discussed, this would be deemed a wise move.

The high level process of creating this architecture will now be discussed, although it is recommended that the referenced publication be used to provide further information. Where areas within the process are present that relate to the provision of business benefit, these shall be discussed, it is not within the scope of this document to provide a full overview of the process.

In order to create a SABSA® security architecture, it is recommended to undertake two stages – the Strategy and Concept phase, where the definition of the Contextual and Conceptual architectures occurs, and then the Detailed design phase. This two-phase approach is recommended due to the need for the buy-in and sign-off from the senior business managers to provide the necessary backing to allow the rest of the work to be undertaken.

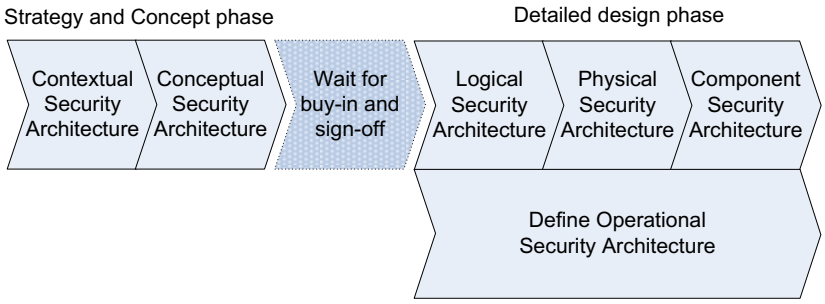



**Figure 4-10 Phases of implementation of SABSA® methodology[193]**

Given all the discussion thus far on the topic of the need to improve perceptions and understanding amongst business managers, it is wise to undertake this activity. This especially so if the previous steps addressing the perception and understanding issues have been undertaken. This activity will further serve to provide an impression within the business of the provision of security that is relevant to the needs of the business.

Once the necessary buy-in and sign-off have been obtained, the rest of the architecture can be defined. An example of the components of the fully defined security architecture is provided overleaf. In line with the approach employed by the benefits management methodology, it can be seen from this diagram that the SABSA® methodology does not define the products and/or tools to be used until the desired functionality is defined. This can greatly assist in both product

selection and the maximising of efficiency, whilst still providing a direct linkage to the business driver requiring the use of the product and/or tool.

During the contextual architecture definition, the business drivers need to be understood. This is, in part facilitated by the provision a business attributes, where a selection of attributes is made from a list deemed to be common to organisations.

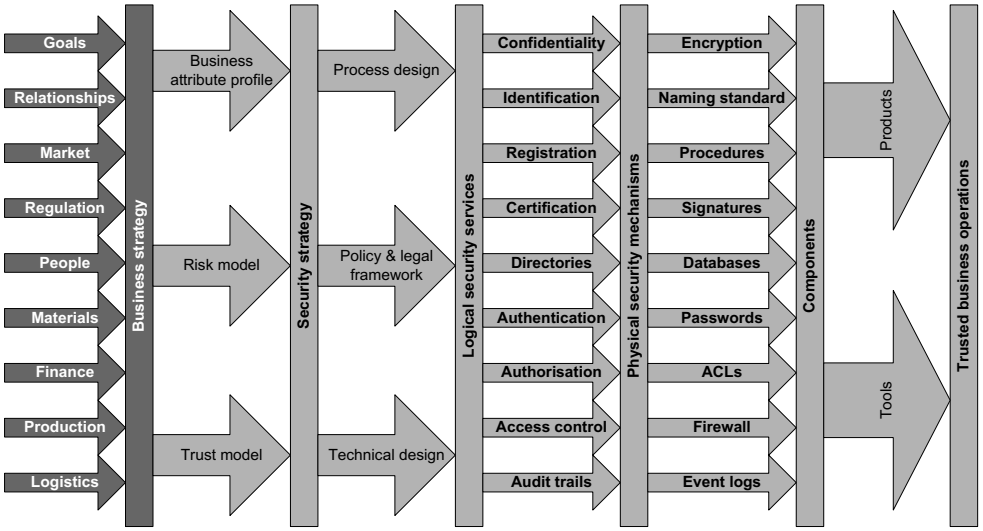



**Figure 4-11 Sample areas of SABSA® architecture[194]**

This list is then used as the basis of a risk assessment process to allow the creation of a threats database. The threats database includes a mapping to the Basel II threat domains introduced previously within the discussion regarding threats within this document.

The provision of a method by which the risks relevant to organisations is welcome as the lack of risk assessment has been alluded to both in the previous section and elsewhere within this document as being of concern. The utilisation of the threat domains from Basel II further increases the relevance both of the methodology, and the ability to

effectively undertake corporate governance for those organisations affected by this accord.

The conceptual design concerns itself with the laying of the foundations of the multi-layered approach to security, the facility to conduct efficient incident processing, the services required to secure applications (Including middleware and data services), the security required within the network and directory services and defines the PKI strategy and the notion of security domains of trust.

All of these areas would have the potential to address the majority of the threats previously discussed. The challenges to the traditional view of perimeter security have already been discussed, and these concepts are also being discussed by the Jericho Forum[195], which is currently discussing the concept of deperimeterisation. This concept has the ability to reduce the risk from the 'hard shell, soft centre' security architecture of most networks. This can provide the opportunity to reduce the risks to a level where technologies that have huge financial benefits to organisations but are deemed of extreme risk to the traditional network security architectures deployed can be adopted (eg VoIP, Instant Messaging). This approach would also reduce the risk from people being subjected to a directed attack designed to circumvent these traditional technological measures.

Once this conceptual view of the architecture has been completed, the logical architecture is defined. The logical architecture provides more substance to the foundations set by the conceptual architecture and especially concerns itself with the definition of policies to be used throughout the architecture, services to provide the activities defined within the conceptual architecture and defines the logical security domains of an organisation.

An overview of the procedures provided within the SABSA® methodology and their placement within the different architectural layers is shown below:

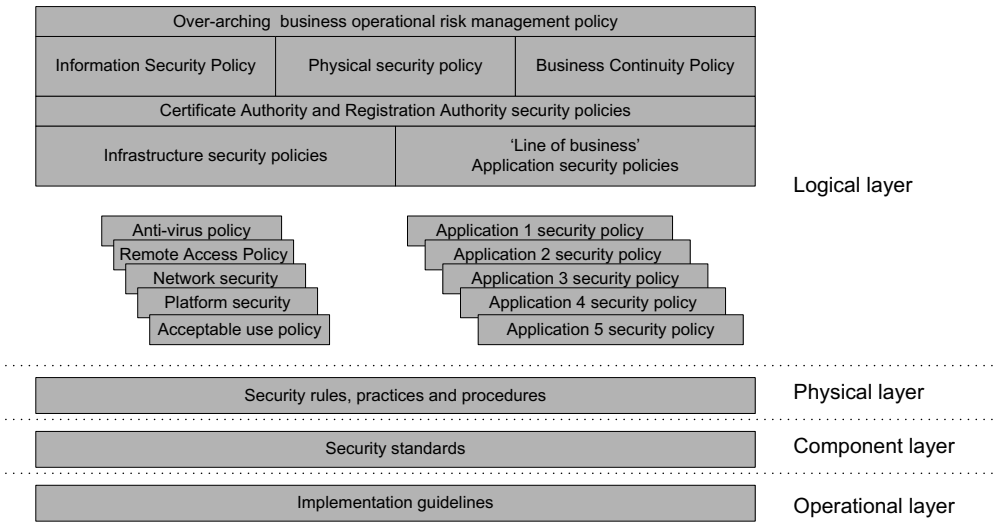



**Figure 4-12 Placement of procedures within architecural layers[196]**

The equal importance given to the information security, physical security and BCP is of note as this again addresses perception issues already discussed. The technological and sociological measures which are commonly implemented throughout organisations are derived from both the information and infrastructure policies, ensuring that all relevant threats should be addressed and that perception issues are minimised.

The definition of the security domains within the logical architecture can allow an understanding of the security controls required, but also the work undertaken to create these logical diagrams can also facilitate a better understanding of the organisation from a business perspective and would deemed to provide the potential to benefit both operational teams and business analysts amongst others. The benefit

that can be derived from the creation of both logical and physical network architecture is increased when taking the system classification method[197] within the operational architecture to ensure that the security requirements of systems hosting applications with different Confidentiality, Integrity and/or Availability (CIA) risks are understood.

The physical security architecture concerns itself with the protection of data, provision of security and cryptographic mechanisms, definition of the security rules, practices and procedures, platform and network security and end user security requirements.

The component architectural layer provides the data structures, defines security tools and products, defines the standards and communications to be used within the organisation.

Finally the operational architecture is defined, defining the operational processes relating to security, risk methodologies, security policy management and monitoring strategies amongst others. Of note here is the definition of a systems-based approach to information classification; this assesses applications based on the risk posed to the CIA risk attributes and then assigns a security policy based on the risk rating. When combined with the logical and physical network diagrams previously mentioned, this provides the facility to simplify controls based on the security requirements of an application. This could allow the placement of applications on systems configured with a defined security configuration, according to the application risk rating, which would increase the security of systems infrastructure by the adoption of hardened builds tailored to the risk environment.

This utilisation of 'least privilege' configurations is a cost-effective way to protect systems and also enhances the abilities of technologies such as IDS if the communications allowed on systems are known. This also allows systems of a less secure configuration to be located in a different logical and/or physical network environment with different controls placed on those systems based on the level of trust associated with them.

## 4.4 Measurement of performance

It has been illustrated through this document that there are issues with regards to measurement of the performance of security within organisations. With better understanding of the operating environment and improved perception and understanding surrounding the usefulness of the security function, the value attributed to the security function would be expected to improve.

It should be understood what is being measured, and is this measurement sufficient? An example could be the measurement of the amount viral detections from an anti-virus solution; what do these infection tell us? Not much due to reasons previously discussed; however if the root cause is able to be measured then the measurement becomes more useful (ie Does the malware depend on a vulnerability within an application or operating system?) in that if this root cause is continually seen month after month, then it could be construed that there is a failing within a security control. To date there is no malware solution that is known to be able to achieve this, so the onus is on the security function to undertake this activity. However, this can be undertaken to a point with the current information available; instead of reporting the top ten infections, report the top five causes. Malware changes so rapidly that the mere measurement of

infections is wholly insufficient to achieve a true understanding of the performance of the security controls.

Pete Wood makes the point that *"statistical data from vendors about security incidents is a poor basis for strategy. This type of data must by definition be skewed (Spin doctored?) to present the vendor's product in the best possible light. Security isn't about how many phishing attacks there are, or how many viruses have emerged this month, or how many web sites have been hacked this year. It's about understanding the threats to your business in the context of the current economic, political and local situation. Vendors generally want people to buy "silver bullets" and lots of them, rather than an homogenous solution (which would be hard to sell and hard to implement). Thus product-based solutions will drive against a "proper" information security infrastructure. Trying to prove that your security strategy is contributing to the business by showing how many viruses you've stopped at the e-mail gateway is dangerous. It limits the execs' view of security and encourages IT security as opposed to information security. We need to change security's position on the enterprise from 'apologetic and appeasing' to 'assertive and high profile'."*

## 4.5 Summary

The issues defined as being of relevance to the perception of security within organisation have been highlighted during the research conducted within this document. It has been shown, however, that the issues can be overcome with some thought. The different issues should be addressed in an order specific to the cultural environment in which the organisation operates.

# 5 Conclusion

This document began by looking at the statement from the 2005 Deloitte security survey regarding the value that security can provide to an organization not being accurately illustrated and that measurement of the performance of the security function is not being conducted.

It has been determined through this document that the purpose of security is to protect against the threats to an organisation. All the research points to organisations not being aware of the threats to their environment, the increase in vulnerabilities that require end-user interaction and the vast majority of attacks being internal but with no changes being made to systems infrastructure/configuration to counter this threat.

The reliance on an outdated view of the network perimeter is allowing companies to assume that their systems are safe behind the perimeter defences when criminal elements are actively attempting to subvert internal staff to gain access to their internal systems using phishing techniques. Companies cannot afford to assume that their internal systems will not become a staging point for attacks.

This reliance will also hinder attempts to adopt cost-saving exercises such as outsourcing of development and the ability to realise efficiencies due to information sharing with business partners and adoption of cost-saving technologies that are not compatible with traditional perimeter-based security architecture.

Whilst the vast majority of organisations feel that they are giving priority to security, the evidence points toward a largely technological approach that provides protection against the perceived external threats but one in which the companies have no confidence with regards to the internal threats. This

reliance on technological controls is also reinforced with all the major surveys on security produced within the past year relating spend on security to the IT budget. This perception of security being seen as a mainly technological function results in it being seen as an overhead rather than a benefit. If not benefits are perceived, then experience shows that often the control is switched off to allow the operation of a 'more useful' technology as a short-term measure that becomes permanent.

Although the security benefits of technological controls are without question, research points toward the need to provide an additional sociological remedy to the threats posed, although there appears to be a reticence from organisations to moving towards this. This could be construed to be due to the exiting controls being perceived as being one-dimensional and providing no usefulness to the organisation. Without a change in the perception towards these controls, and boardroom support, it will be very hard to fully understand the benefits of these controls. The lack of importance given toward elevating the visibility of the security function up to the boardroom, which in turn affects the facilitation of corporate governance, is concerning.

This lack of corporate governance is evident in the culture of regulatory/legislative compliance shown from recent research. This culture does not facilitate true control and instead ensures that companies are continually reacting to new statutes rather than concentrating on generating value.

The measurement of the performance of security within the enterprise would also appear to be insufficient due to a lack of risk assessment relating to the vulnerability to the threats, and a reliance on using vendor-supplied performance metrics which have no relevance to the underlying causes of the incidents and merely serve to provide a justification to spend more on technological controls.

A point of interest is that all of the surveys researched continually related the expenditure on security as a percentage of the IT budget, and the dti security survey referred to information security when it could be deemed that the intention was to research the holistic view of security. The current research available perpetuates the notion of security being a technological measure.

The current research available is therefore deemed to be insufficient to fully determine the issues affecting the security functions. The lack of questioning within the surveys to make an attempt to determine what functions actually report to security managers, the point at which the engagement of security functions in business projects occurs, the perception of security functions from an enabling/inhibiting perspective, the role security functions fulfil within the enterprise, the policies that have been implemented and the approach that organisations take to deal with sociological security issues is disappointing.

This information, combined with a determination of security expenditure in relation to organisational outgoings would give a better picture of the importance given to security within the enterprise. It is intended to continue the research in this area to undertake a survey attempting to understand if the findings derived from the research provide an accurate reflection of current trends within the enterprise.

The issues defined as being of relevance to the perception of security within organisations have been highlighted during the research conducted within this document. It has been shown, however, that these issues can be overcome with some thought. The different issues should be addressed in an order specific to the cultural environment in which the organisation operates. It is also of note that some of the methodologies discussed can take an amount of time to achieve the full benefits and it is feasible that

even partial adoption could improve the value perception sufficiently to allow organisational support to continue with the implementation of the methodologies described within this chapter.

It is recommended that the methodologies discussed be implemented with a view to short, medium and long term implementation schedules.

The involvement of stakeholders and the adoption of the benefits management methodology in security projects in the short term could provide a sufficient fillip to engender sufficient interest in the process to adopt it as the standard practice within the organisation.

In a similar vein, the involvement with stakeholders relating to traditional network security products (eg IDS) could show the operational benefits of undertaking the operational understanding required to obtain effectiveness from these products.

The assessment of all new applications according to the system classification method in the medium terms could allow enough statistics to be gathered to show the financial benefits of ensuring that only data from applications with an availability risk are supported by a backup structure to provide rapid retrieval. Given the increase in business intelligence initiatives, this approach could also facilitate the reduction in 'unstructured data' being processed by these systems whilst providing an additional benefit of being able to better secure the investment made in these solutions.

Similarly, the undertaking of the definition of a remote access architecture to SABSA® principles in the medium term, for example, could exhibit the agility of businesses to communicate with new partners or outsource

business functions to generate sufficient support from the business to undertake the implementation of a complete security architecture.

The intention of this document was to show that value and performance of security functions can be exhibited to the enterprise through the utilisation of the Benefits Management and SABSA® methodologies amongst others. It is felt that utilisation of these techniques has sufficiently proven that value in non-financial terms can be shown and that the benefits of a well-structured security function are of great importance to the future prosperity of business functions within the enterprise.

# 6 References


4 – Cappelli, D Keeney, M Kowalski, E Moore, A and Randazzo, M (2004), *'Insider Threat Study: Illicit Cyber Activity in the Banking and Financial Sector'*, US Secret Service and CERT co-ordination centre

http://www.secretservice.gov/ntac/its_report_040820.pdf (10 Jan 2004)

5 – Anon, (2004), 'Anatomy of a 419 scam', *The Register*, http://www.theregister.co.uk/2004/07/09/419_scam_anatomy/ (10 Jan 2004)

6 – Anon, 'Symantec Internet Security Threat Report Identifies More Attacks Now Targeting e-Commerce, Web Applications', *Symantec* http://www.symantec.com/press/2004/n040920b.html (10 Jan 2004)

7 – Leyden, J 'Click her to become infected', *The Register*, http://www.theregister.co.uk/2004/09/22/opt-out_exploit/ (10 Jan 2004)

8 – Anon, 'Policy on Transfer of Registrations between Registrars', *the Internet Corporation for Assigned Names and Numbers* http://www.icann.org/transfers/policy-12jul04.htm (10 Jan 2004)

9 – Anon, 'Transfer Dispute Resolution Policy'*, the Internet Corporation for Assigned Names and Numbers* http://www.icann.org/transfers/dispute-policy-12jul04.htm (10 Jan 2004)

10 – Anon, 'Spyware infiltration rises in corporate networks, but Webroot survey finds companies still neglect threat', *Webroot* http://www.webroot.com/company/pressreleases/20041027-spysweeper-corp/ (10 Jan 2004)

11 – Leyden, J 'Sophos in porn dialler row with UK developer', *The Register,* http://www.theregister.co.uk/2004/09/30/sophos_porn_dialler_row/ (10 Jan 2004)

12 – Anon, 'Detection of adware', *Sophos* http://www.sophos.co.uk/support/knowledgebase/article/1642.html (10 Jan 2004)

13 – Anon, 'Welcome Slashdot, Bugtraq, CNET et al', *Easynews* http://www.easynews.com/virus.html (10 Jan 2004)

14 – Howes, E 'The Spyware Warrior Guide to Anti-Spyware Testing', *Spywarewarrior.com* http://spywarewarrior.com/asw-test-guide.htm#overview (10 Jan 2004)

1 – Bainbridge D, (2004), 'Introduction to Computer Law - Fifth Edition', *Pearson Education Limited*, Harlow, pp105-106

2 – Bainbridge D, (2004), 'Introduction to Computer Law - Fifth Edition', *Pearson Education Limited*, Harlow, pp103

3 – Laurence, GA Loeb, MP (2005), '2005 CSI/FBI Computer Crime and Security Survey', *CSI Institute,* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf (4 Jun 2006)

4 – Great Britain, 'Computer Misuse Act 1990', *Crown*, http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm (4 Jun 2006)

5 – Great Britain, 'Data Protection Act 1998', *Crown*, http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm (4 Jun 2006)

6 – Information Commissioner, 'The Employment Practices Data Protection Code Part 3 Monitoring at work', *Information Commissioner*, http://www.privacydataprotection.co.uk/pdf/employment_code_of_practice.pdf (4 Jun 2006)

7 – Great Britain, 'Human Rights Act 1998', *Crown*, http://www.opsi.gov.uk/ACTS/acts1998/19980042.htm (4 Jun 2006)

8 – Reed, M, 'Raphael Gray – Curador', *M J Reed Solicitors,* http://www.mjreedsolicitors.co.uk/index.php?option=com_content&task=view&id=14&Itemid=2 (4 Jun 2006)

9 – Barker, C Wearden, G, 'Tsunami 'hacker' found guilty', *Silicon.com,* http://management.silicon.com/government/0,39024677,39153121,00.htm (4 Jun 2006)

10 – Anon, 'Payment Card Industry Data Security Standard', *VISA,* http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf (4 Jun 2006)

11 – Bainbridge D, (2004), 'Introduction to Computer Law - Fifth Edition', *Pearson Education Limited*, Harlow, pp197-199

12 – Anon, 'PCI Compliance: Are You Onboard?', *Tripwire.com,* http://www.tripwire.com/files/literature/white_papers/SBPCI1.pdf (4 Jun 2006)

13 – Anon, 'Dental practice refused credit licence', *Office of Fair Trading,* http://www.oft.gov.uk/News/Press+releases/2006/05-06.htm (4 Jun 2006)

14 – Anon, 'OWASP Top Ten Project', *OWASP.org,* http://www.owasp.org/index.php/OWASP_Top_Ten_Project (4 Jun 2006)

15 – Anon, 'Web Application Security Consortium: Threat Classification', Web Application Security Consortium, http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.pdf (4 Jun 2006)

16 – Bainbridge D, (2004), 'Introduction to Computer Law - Fifth Edition', *Pearson Education Limited*, Harlow, pp412-415

17 – Great Britain, 'Copyright, Designs and Patents Act 1988', *Crown*, http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm (4 Jun 2006)

18 – Bainbridge D, (2004), 'Introduction to Computer Law - Fifth Edition', *Pearson Education Limited*, Harlow, pp414

19 – Anon, 'Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution', *Microsoft*, http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx (4 Jun 2006)

20 – Anon, 'Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution', *Microsoft*, http://www.microsoft.com/technet/security/bulletin/ms06-001.mspx (4 Jun 2006)

31 - http://www.theregister.co.uk/2006/06/27/usb_drives_security_threat/

33 - http://www.compuware.co.uk/pressroom/news/03072006.htm

90 - http://www2.csoonline.com/blog_view.html?CID=22705

95 - http://www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_en/intelligence_reports/june_2006/DA_155198.chp.html

111 - http://www.zdnet.com.au/blogs/securifythis/soa/Why_popular_antivirus_apps_do_not_work_/0,39033341,39264249,00.htm

# 7 Bibliography


Anon, (2004), 'Anatomy of a 419 scam', *The Register*, http://www.theregister.co.uk/2004/07/09/419_scam_anatomy/ (10 Jan 2004)

Anon, 'Symantec Internet Security Threat Report Identifies More Attacks Now Targeting e-Commerce, Web Applications', *Symantec* http://www.symantec.com/press/2004/n040920b.html (10 Jan 2004)

Anon, 'Policy on Transfer of Registrations between Registrars', *the Internet Corporation for Assigned Names and Numbers* http://www.icann.org/transfers/policy-12jul04.htm (10 Jan 2004)

Anon, 'Transfer Dispute Resolution Policy'*, the Internet Corporation for Assigned Names and Numbers* http://www.icann.org/transfers/dispute-policy-12jul04.htm (10 Jan 2004)

Anon, 'Spyware infiltration rises in corporate networks, but Webroot survey finds companies still neglect threat', *Webroot* http://www.webroot.com/company/pressreleases/20041027-spysweeper-corp/ (10 Jan 2004)

Anon, 'Detection of adware', *Sophos* http://www.sophos.co.uk/support/knowledgebase/article/1642.html (10 Jan 2004)

Anon, 'Welcome Slashdot, Bugtraq, CNET et al', *Easynews* http://www.easynews.com/virus.html (10 Jan 2004)

Cappelli, D Keeney, M Kowalski, E Moore, A and Randazzo, M (2004), *'Insider Threat Study: Illicit Cyber Activity in the Banking and Financial Sector'*, US Secret Service and CERT co-ordination centre

http://www.secretservice.gov/ntac/its_report_040820.pdf (10 Jan 2004)

Gordon, L Loeb, M Lucyshyn, W and Richardson, R (2004), *'2004 CSI/FBI Computer Crime and Security survey'*, Washington, Computer Security Insitute.

http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf (10 Jan 2004)

Hall, L Stride, C Turgoose, C and Warr, J (2004), *'People and Technology – Is HR getting the best out of IT?'*, London, Chartered Institute of Personnel and Development.

http://www.cipd.co.uk/NR/rdonlyres/328BDDEC-2C70-4120-92E9-A4EE6E86090D/0/3081peopletechsurv04.pdf (10 Jan 2004)

Howes, E 'The Spyware Warrior Guide to Anti-Spyware Testing', *Spywarewarrior.com* http://spywarewarrior.com/asw-test-guide.htm#overview (10 Jan 2004)

Leyden, J 'Click her to become infected', *The Register*, http://www.theregister.co.uk/2004/09/22/opt-out_exploit/ (10 Jan 2004)

Leyden, J 'Sophos in porn dialler row with UK developer', *The Register,* http://www.theregister.co.uk/2004/09/30/sophos_porn_dialler_row/ (10 Jan 2004)

Anon, 'Buffer Overrun in JPEG Processing (GDI+) Could Allow Code Execution', *Microsoft*, http://www.microsoft.com/technet/security/bulletin/ms04-028.mspx (4 Jun 2006)

Anon, 'Dental practice refused credit licence', *Office of Fair Trading,* http://www.oft.gov.uk/News/Press+releases/2006/05-06.htm (4 Jun 2006)

Anon, 'OWASP Top Ten Project', *OWASP.org,* http://www.owasp.org/index.php/OWASP_Top_Ten_Project (4 Jun 2006)

Anon, 'Payment Card Industry Data Security Standard', *VISA,* http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_PCI_Data_Security_Standard.pdf (4 Jun 2006)

Anon, 'PCI Compliance: Are You Onboard?', *Tripwire.com,* http://www.tripwire.com/files/literature/white_papers/SBPCI1.pdf (4 Jun 2006)

Anon, 'Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution', *Microsoft*, http://www.microsoft.com/technet/security/bulletin/ms06-001.mspx (4 Jun 2006)

Anon, 'Web Application Security Consortium: Threat Classification', Web Application Security Consortium, http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.pdf (4 Jun 2006)

Bainbridge D, (2004), 'Introduction to Computer Law - Fifth Edition', *Pearson Education Limited*, Harlow, pp105-106

Barker, C Wearden, G, ‘Tsunami 'hacker' found guilty’, *Silicon.com,* http://management.silicon.com/government/0,39024677,39153121,00.htm (4 Jun 2006)

Great Britain, ‘Computer Misuse Act 1990’, *Crown*, http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm (4 Jun 2006)

Great Britain, ‘Copyright, Designs and Patents Act 1988’, *Crown*, http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm (4 Jun 2006)

Great Britain, ‘Data Protection Act 1998’, *Crown*, http://www.opsi.gov.uk/ACTS/acts1998/19980029.htm (4 Jun 2006)

Great Britain, ‘Human Rights Act 1998’, *Crown*, http://www.opsi.gov.uk/ACTS/acts1998/19980042.htm (4 Jun 2006)

Information Commissioner, ‘The Employment Practices Data Protection Code Part 3 Monitoring at work’, *Information Commissioner*, http://www.privacydataprotection.co.uk/pdf/employment_code_of_practice.pdf (4 Jun 2006)

Laurence, GA Loeb, MP (2005), ‘2005 CSI/FBI Computer Crime and Security Survey’, *CSI Institute,* http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf (4 Jun 2006)

Reed, M, ‘Raphael Gray – Curador’, *M J Reed Solicitors,* http://www.mjreedsolicitors.co.uk/index.php?option=com_content&task=view&id=14&Itemid=2 (4 Jun 2006)

# 8 Glossary

ACL
ICT
IDS
IPS
MiFID

## Appendix I – Overview of Top Ten Viral Threats (2003 to date)

Top 10 viral threats – 2006 to date

| Name | Mass Mailer | Steals confidential information | Kills AV and FW services | Uses IE vuln | Uses O/S vuln | Keylogger/ Backdoor | Botnet programs | DoS attempt |
|---|---|---|---|---|---|---|---|---|
| Sober-Z | X | | X | | | X | | |
| Netsky-P | X | X | X | | | | | |
| Zafi-B | X | X | X | | | | | |
| Nyxem-D | X | | X | | | | X | |
| Mytob-FO | X | | X | | | X | X | |
| Netsky-D | X | X | X | | | | | |
| Mytob-BE | X | X | X | | X | X | X | |
| Mytob-EX | X | | X | | | X | X | |
| Mytob-AS | X | X | X | | X | X | X | |
| Bagle-ZIP | X | X | X | | | X | | |

Viral threats marked in RED were present in the previous year's top ten threats produced by Sophos.

Top 10 viral threats – 2005

| Name | Mass Mailer | Steals Confidential information | Kills AV and FW services | Uses IE vuln | Uses O/S vuln | Keylogger/ Backdoor | Botnet programs | DoS attempt |
|---|---|---|---|---|---|---|---|---|
| Zafi-D | X | X | X | | | X | | |
| Netsky-P | X | X | X | | | | | |
| Sober-Z | X | | X | | | X | | |
| Sober-N | X | X | X | | | | | |
| Zafi-B | X | X | X | | | | | |
| Mytob-BE | X | X | X | | X | X | X | |
| Mytob-AS | X | X | X | | X | X | X | |
| Netsky-D | X | X | X | | | | | |
| Mytob-GH | X | | X | | | X | X | |
| Mytob-EP | X | | X | | | X | X | |

Viral threats marked in RED were present in the previous year's top ten threats produced by Sophos.

Top 10 viral threats – 2004

| Name | Mass Mailer | Steals confidential information | Kills AV and FW services | Uses IE vuln | Uses O/S vuln | Keylogger/ Backdoor | Botnet programs | DoS attempt |
|---|---|---|---|---|---|---|---|---|
| Netsky-P | X | X | X | | | | | |
| Zafi-B | X | X | X | | | X | | |
| Sasser-A | | | | | X | X | | |
| Netsky-B | X | X | X | | | | | |
| Netsky-D | X | X | X | | | | | |
| Netsky-Z | X | X | | | | X | | X |
| MyDoom-A | X | X | | | | X | | X |
| Sober-I | X | X | | | | | | |
| Netsky-C | X | X | X | | | | | |
| Bagle-AA | X | X | X | | | X | | |

Viral threats marked in RED were present in the previous year's top ten threats produced by Sophos.

Top 10 viral threats – 2003

| Name | Mass Mailer | Steals Confidential information | Kills AV and FW services | Uses IE vuln | Uses O/S vuln | Keylogger/ Backdoor | Botnet programs | DoS attempt |
|---|---|---|---|---|---|---|---|---|
| Sobig-F | X | X | X | | | X | X | |
| Blaster-A | | | | | X | X | X | X |
| Nachi-A | | | | | X | X | | |
| Gibe-F | X | X | X | | X | | | |
| Dumaru-A | X | X | | | | X | | |
| Sober-A | X | X | | | | | | |
| Mimail-A | X | X | | X | X | | | |
| Bugbear-B | X | X | X | | X | X | | |
| Sobig-E | X | X | | | | X | X | |
| Klez-H | X | X | X | X | | | | |

Viral threats marked in RED were present in the previous year's top ten threats produced by Sophos.

## Appendix II – Overview of Microsoft Vulnerabilities

| | 2006 to date | | 2005 | | 2004 | | 2003 | |
|---|---|---|---|---|---|---|---|---|
| **Category** | **Total** | **Critical** | **Total** | **Critical** | **Total** | **Critical** | **Total** | **Critical** |
| Operating System | 37 (37.4%) | 17 (51.4%) | 52 (60.5%) | 20 (38.5%) | 52 (65.0%) | 15 (28.9%) | 30 (41.1%) | 17 (56.7%) |
| Application | 40 (40.4%) | 33 (82.5%) | 18 (20.9%) | 8 (44.4%) | 15 (18.8%) | 7 (46.7%) | 27 (37.0%) | 6 (22.2%) |
| Internet Explorer | 29 (29.3%) | 16 (55.2%) | 28 (32.6%) | 19 (67.9%) | 23 (28.8%) | 12 (52.2%) | 20 (27.4%) | 16 (80%) |
| Wormable | 13 (13.1%) | 6 (46.1%) | 19 (22.1%) | 11 (57.9%) | 18 (22.5%) | 10 (55.6%) | 12 (16.4%) | 10 (83.3%) |
| User interaction required | 86 (86.9%) | 56 (65.1%) | 51 (59.3%) | 32 (62.8%) | 49 (61.3%) | 19 (38.8%) | 43 (58.9%) | 25 (58.1%) |

Explanation of categories:

*Operating System* – Affects a core component of the Microsoft operating system, excluding the Internet Explorer component, which would typically be present without installation of further products.

*Application* – Affects a non-standard server component (ie Exchange, Internet Information Server) or other Microsoft Application (eg MS Office).

*Internet Explorer* – Affects a component of the Internet Explorer browsing software, or exploits require Internet Explorer as an attack vector.

*Wormable* – The vulnerability is severe enough to allow remote execution of code with system level privileges or allows remote privilege escalation without any intervention by a human.

*User interaction required* – The vulnerability requires user intervention to exploit the vulnerability

## Appendix III – Interview with Peter Wood

Name: *"Peter Wood"*

Company: *"First Base Technologies"*

Position held: "*Partner, Chief of Operations"*

Security experience: *"18 years in present post, previously IT infrastructure and communications".* Peter is also an experienced security speaker and runs the White Hats security interest group

Date of interview: 14th August 2006

Q Do you feel that the new legislation such as Basel II, MiFID and Sarbanes-Oxley will change the way that enterprises view the value of the security function? If so, what changes do you envisage?

A *"I fear this will reinforce senior executives' view of security as a "necessary evil", since most entrepreneurs object to external "interference". However, it is likely to embed security more deeply in standard business processes which must help. Clever security managers may take the opportunity to convince execs of the value of security in this context, but it will be dependent on the individuals concerned. Often security people are not wholly realistic about business practices or ordinary staff's attitudes and motivators, so they must change their own attitudes in order to take advantage of this change in the corporate landscape."*

Q Do you feel that CISO's have the visibility within the enterprise in terms of the level of seniority they possesses? What effect does this have on the business perception of the security function?

A *"I still have yet to meet a CISO. They must exist if you believe the press, and they certainly appear to exist in the USA, but not in our client base."*

Q Do you feel that enough non-technological security functions are reporting to the CISO function? If not, do you feel that this contributes to the value perception within the enterprise?

A *"Where there is someone with a CISO-like role (albeit usually lower down the hierarchy than C-suite in our client base) then they are too often IT security rather than information security, so the answer is "no". This must change if real security is going to emerge as part of "business as usual". Most firms just don't understand this."*

Q Do the different roles that the security function is believed to provide throughout different organisations (eg Risk, IT and Compliance functions) contribute to the challenges that security functions have in showing value? If so, in what way?

A *"Yes. It's hard to offer cross-industry comparatives when there's no single model of implementing security. And it's hard to get senior execs to talk to each other about security if most are playing another role which they view as their 'real' role (e.g. CFO, CIO, IT Director, and Finance Director). Industry has a long way to go before security is seen as one of the key supporting pillars of commerce, equivalent to, but separate from Finance, IT, etc. It's only recently that IT has been separated from Finance in some firms (and in some large firms it still hasn't been)."*

Q How do you feel that security functions are primarily perceived within the enterprise, enablers or inhibitors? In what ways can this perception affect the engagement of the security function in projects?

A *"Inhibitors almost without exception. This is exacerbated by the attitude of many security professionals who are frequently pious, unrealistic and commercially naive. Security must leave behind the BS / ISO mindset and become commercially literate and able to speak to entrepreneurs and the C-suite on their own terms."*

Q Do you feel that enough is being done by security functions to understand the perspective of the end users community? If not, why do you feel that this is the case?

A *"No. Again the pious and unrealistic attitude of a lot of security professionals makes this a big problem. Couple that with a very limited understanding of marketing and training (which are essential to implementing change in staff and corporate culture) and you have a poor outlook."*

Q Do you feel that the certifications within the security industry are sufficient to provide a benchmark for employers to gauge the competence of security professionals?

A *"Not really. CISSP is the closest we have to a certification that employers can understand, but really it's not an ideal measure IMHO. Most tests are good for people who do well at tests and CISSP is no different. An MSc in Information Security might be better - having seen one course close up, I'm definitely not convinced!"*

Q Do you feel that security professionals will have to undertake business certifications such as the MBA or CIMA to provide better value to the enterprise in the future?

A *"I don't know enough about MBA and I've never heard of CIMA. Practical, focused commercial training courses would seem to be the way to go though. I attended several leadership, marketing, sales and negotiation courses in my early career and they helped me considerably in structuring and presenting my case. However I guess large corporations run in a particular way (which I never understand) and if an MBA would help a security professional to understand this and to survive at the upper levels then it would be a good idea."*

Q Do you feel that security associations provide adequate value to their members to in turn provide value to the enterprise?

A *"To some degree. BCS-ISSG, BCS-IRMA and IACA do good stuff at a local level on specific topics. Mostly there doesn't appear to be sufficient co-ordinated training on the breadth of topics needed. The Institute of Directors should be able to organise something appropriate but (cynically) I believe they're too interested in an old boys' network to look for the right people to deliver it."*

Q Do you feel that security functions could be seen in a more favourable light by creating security architectures aligned with business drivers? What challenges do you see in the adoption of such strategies within the enterprise?

A *"Of course! The biggest challenge is getting business people interested in security and security people to understand the entrepreneurial mindset. Bridge that chasm and you're in with a chance."*

Q Do you feel that security functions adequately address information security issues? What affect does this have on the value perception?

A *"No. The focus is strongly on IT security and specific controls therein. This makes security part of the IT function, which in turn is still seen as an overhead."*

Q Does the lack of defined policies and/or procedures affect the way that security functions are perceived within the enterprise? If so, in what way?

A *"Yes. Where there are policies and procedures, there are not part of an internal marketing and training campaign, so that staff quickly forget that they exist. Then the only person who reads them is the person who wrote them. IT people (and all staff really) are excellent at making up their own procedures for what they believe is the best result for their employer. As a result, firms end up with a large number of conflicting and home-made processes which are uncoordinated and sometimes plain wrong."*

Q Do you feel that a lack of understanding of the threats and the failure to communicate them to business in terms they understand hampers the way that the security function is seen within the enterprise?

A *“Yes again. Emphatically. Senior execs get their perception of threats from a mixture of ‘common sense’ (ie what seems likely to them) and what the press tell them. This distorts the picture of the real threats and leaves the security professional trying to sell a different story to an exec who already thinks they know the answer. (eg “why would anyone want to hack our site?”)”*

Q Do security professionals spend enough time educating people on the wider benefits of their work? Can this be hampered on the focus on technological solutions by the enterprise?

A “*No, not at all. See all references above to the lack of security professionals’ skills in marketing, selling and communication. Train the security people to be more ‘peoples people’ and the problem will recede.”*

Q Do you feel that the vendors within the security industry drive the typical metrics that are employed within enterprises as a method of performance? Are these measurements relevant to providing a measurement of the success of the security function and what other methods could be employed?

A *"Statistical data from vendors about security incidents is a poor basis for strategy. This type of data must by definition be skewed (Spin doctored?) to present the vendor's product in the best possible light. Security isn't about how many phishing attacks there are, or how many viruses have emerged this month, or how many web sites have been hacked this year. It's about understanding the threats to your business in the context of the current economic, political and local situation. Vendors generally want people to buy "silver bullets" and lots of them, rather than an homogenous solution (which would be hard to sell and hard to implement). Thus product-based solutions will drive against a "proper" information security infrastructure. Trying to prove that your security strategy is contributing to the business by showing how many viruses you've stopped at the e-mail gateway is dangerous. It limits the execs' view of security and encourages IT security as opposed to information security. We need to change security's position on the enterprise from ‘apologetic and appeasing’ to ‘assertive and high profile’.”*

Q Do enterprises typically change their perception of the value that the security function provides after an incident?

A *“Always. More incidents = more investment = sometimes better security. But for a limited period. Execs have goldfish memories and people generally don’t want to think about disasters, criminal activities etc.”*