

# **Information Security Officer's Role & Responsibilities**

Security Management: Assignment 1

*Due Date 4<sup>th</sup> November*

Peter Davies B.Sc - 05004306

MSc Information Security & Computer Crime

## **Abstract**

This report will critically discuss the role and responsibilities of the Information Security Officer. It will examine the history of information security and describe how applicable an ISO's role is within an organisation.

It will systematically critically assess the approaches and standards related to the implementation and management of security within an organisation, based on the information taught and researched during the MSc Information Security and Computer Crime course at the University of Glamorgan.

## Contents

Abstract.....	2
Contents .....	3
Introduction.....	4
The Information Security Officer .....	5
Security History .....	6
Role.....	8
Responsibilities.....	10
Risk Management .....	11
Threat Analysis .....	12
Development of Policies.....	14
Standards & Models.....	15
The Laws.....	16
Incident Management.....	17
Awareness and self learning .....	18
Application to Business .....	19
Conclusions.....	20
Background Reading.....	22
White Papers & Reports.....	22
Websites.....	22
Magazines .....	22
Journals .....	23
References.....	24

## Introduction

Information of any type can be the most valuable asset to a business. So the Information Security Officer (ISO) is responsible for the protection of these corporate assets<sup>1</sup>.

Deloitte's 2004 Global Security Survey<sup>2</sup> revealed that 83 percent of survey respondents acknowledged that their systems had been compromised in the past year, compared to 39 percent in 2003. Furthermore, 40 percent of respondents whose systems were attacked said they sustained financial losses.

The ASIS Online<sup>3</sup> organisation observes this loss of business and tries to address the issue by creating various guidelines aimed at the corporate information security officer. They comment:

*“In an age when information is king, a company’s very survival may hinge on its secrets.”*

If the security officer does not have the aptitude and awareness to make informed decisions regarding a company’s security requirements, or a clear understanding of the organisation’s business, they cannot develop and implement effective policies. The roles and responsibilities given to an ISO will be discussed further in this report.

## **The Information Security Officer**

When discussing the roles and responsibilities of an Information Security Officer, we must also consider the possibility that an organisation might not need an ISO. The question is not that organisations do not need security guidance more that the responsibilities have been spread amongst the other departments.

It is also fair to say that the majority of small businesses are unlikely to have somebody in the information security role. This is either due to poor management or the assumption that it will be dealt with by the IT department. If a specific security role within a small organisation is not established, the responsibilities are often given to the most technical members of the team.

The Information Security Officer is employed within an organisation to perform core duties such as assessing risk, developing security and continuity plans, and ensuring there is a proven technique for incident management. More importantly, the ISO is required to have a deep understanding of the organisation, successfully educating the staff and management of security issues in their relevant departments.

An ISO will help an organisation in preparation for an inevitable attack, providing solutions that will keep the business in operation whilst the incident is being managed (business continuity plans). In the long-run, it will save the organisation from losing money and unnecessary system downtime. This will be achieved through implementing policies and helping it comply with legislation such as the Data Protection Act (concerned with information storage), and the Computer Misuse Act (what employees can and cannot do in the workplace).

## ***Security History***

In the early 1980's computer equipment was large and very expensive. Because of the high value of the equipment organisations would go to great lengths to protect them.

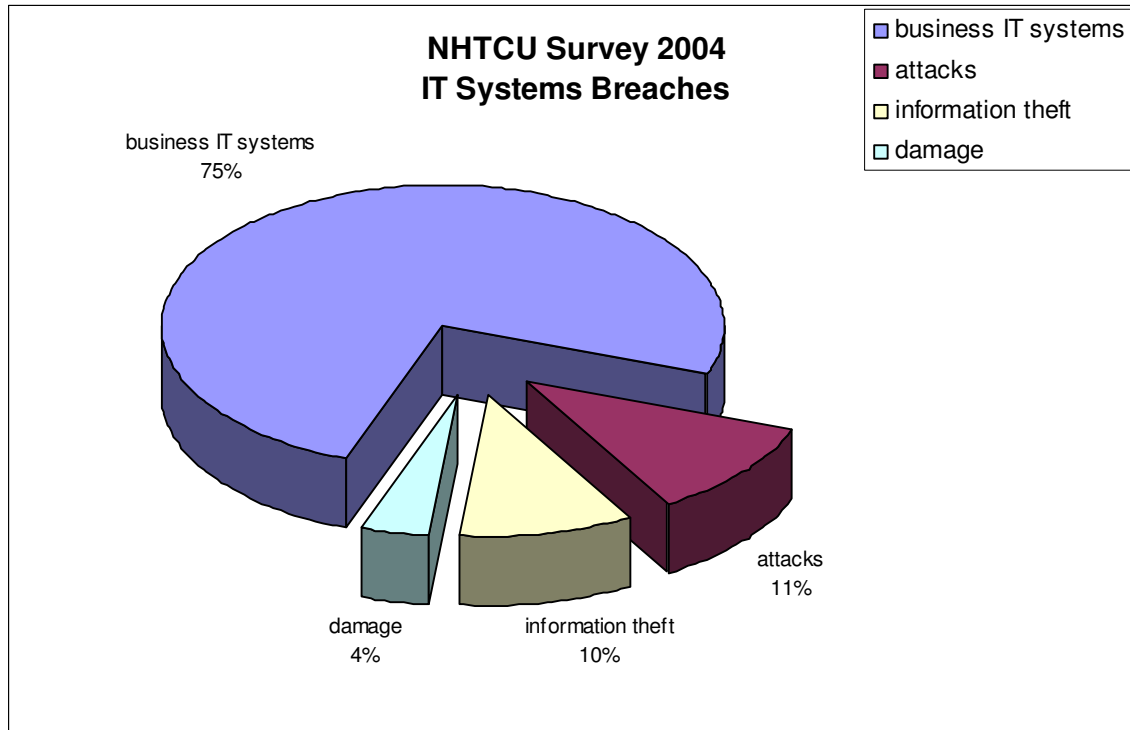
The problem then arose that more and more computers were being inter-connected using networks. As networks were becoming more common place, businesses began to see the introduction of new security threats.

For example, in November 1988, Robert Morris<sup>4</sup> created a self-replicating program (called a 'worm') that spread itself from computer to computer, exploiting various security holes in the Unix operating system. This was the first case to use the Computer Fraud and Abuse Act of 1984 (U.S. law – often referred to as CFAA), and subsequently Morris was convicted and received 3 years probation.

His worm served as a wake-up call to the computer security world. The outcome of which was the formation of CERT, an organisation with the purpose of being a central point of contact for reporting computer security incidents, and today, a core information source for an ISO to use in the event of a security incident.

In recent years, the public has become increasingly conscious of computer viruses and virus-like programs that can self-replicate and spread among computers. The Morris worm differed from earlier viruses (which primarily attacked personal computers) in that it was the first to use networks to spread, on its own, to other vulnerable computer systems.

According to research by the National High Tech Crime Unit (NHTCU), 11 percent of businesses had their IT systems breached by hackers and former employees last year. A further 10 percent of businesses had information stolen from their computer network, and 4 percent had systems damaged or sabotaged.<sup>5</sup>

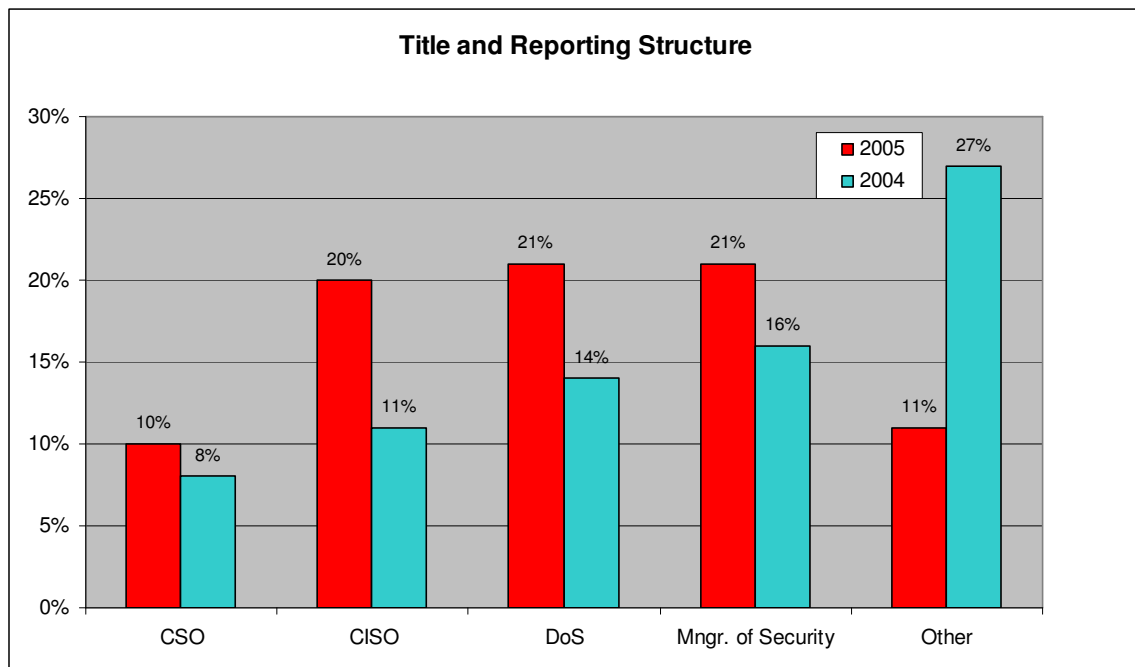


Quoting statistics is an obvious way of bringing attention to the magnitude of the Information Security Officers job. So, given these figures, a security officer can statistically say that in a small company of just 10, at least one of those employees will attempt to crack the organisations IT systems.

The solution (or at least deterrence) is to implement policies and rules that employees must follow, and this report assesses the various approaches and evaluates their features.

## Role

As described earlier, the primary goal of an Information Security Officer is to protect the assets of an organisation. This role comes in many guises, and emerging at various levels within an organisation's operational hierarchy. For example, the Americans use the title Chief Information Security Officer (CISO) which deals with environmental threats as well as computer security. Here in the UK we also have, amongst many, Director of Security (DoS), Corporate Security Officer (CSO) and Information Security Manager (ISM)<sup>6</sup>.



The table above is based on a series of statistics by a CSO Research Series report called *The State of the CSO* (Hanson, J, 2005). It shows the increase in number of designated security individuals being appointed to specific roles between 2004 and 2005. An interesting contrast shows prior to 2005, where staff responsible for security had different or unclassified security job titles. By 2005 these unspecified role titles have changed to specified titles. This indicates that an increase in security based roles globally has led to organisations classifying individuals into recognised security orientated roles. This statement is confirmed by further results in the same report showing that 71 percent of CSO's, CISO's and DoS's are the first people in their organisation to hold their job title.

All of the aforementioned job titles primarily involve protecting a business and its assets, whether it's environmental and/or computer based.

Another key issue is where the ISO sits within an organisation. Some would argue that they should belong in the IT department, but often there is a conflict of interest regarding policies and methods already in place. A recent research report by CSO Online about *The*

*State of Information Security in 2005* indicates that 58 percent of the funding for information security comes from the IT department<sup>7</sup>. The argument being that if the IT department is paying for the resources of an ISO, they should have some management control.

The recommended organisational position would ideally be reporting directly to the Board of Directors (or major stakeholders) and sit at the same level as the IT department. This allows the ISO to create and implement policies from the ground-up, with enough authority to action any requirements. This implies that they would technically get their own budget, although it is likely that other departments will still provide funding as information security covers all aspects of the organisation (e.g. legal, marketing, human resources).

The greatest resistance to change will typically come from the IT department which usually considers its own role as being responsible for such activities. This, though, does not make them qualified to perform the role and duties of the ISO.

So, in summary, the ISO's position within the organisation is often an indicator of the commitment of the management towards security within the business. The higher the security officer in the hierarchy, the greater the liaison will be with the business management structure and it is likely that the company will place a higher value on its security.

## ***Responsibilities***

Depending on the type of business or the size of the organisation, the core duties given to an Information Security Officer may include:

1. assessing risk and evaluating the current security requirements
2. developing an information security plan
3. developing a business continuity plan (disaster preparedness efforts)
4. incident management (response to security incidents and alarms)

The following description of the requirements of an applicant was placed in a recent classified jobs section in a security magazine<sup>6</sup>. It describes the requirements for an experienced Information Security Officer, and encompasses the four key duties listed above amongst other organisational related needs:

- *Directs, manages, plans and administers the operational and administrative activities associated with the running of the IT security department.*
- *Develops, implements security standards, procedures and guidelines for multiple platforms and diverse systems environments.*
- *Reviews the development, testing and implementation of security plans, products and controls techniques*
- *Identifies and accesses IT security risk/ exposure on new and existing infrastructure Investigates and recommends appropriate corrective actions for IT security incidents.*
- *Develops and maintains security policies, controls and their compliance.*
- *Analyses security incidents and escalation of security events.*
- *Liaises with customers with regards to information security incidents.*
- *Studies the proliferation of viruses; prevent hacker intrusion.*
- *Conducts active penetration tests; discovers vulnerabilities in information systems.*

This job description seems typical of most UK security related appointments. You can deduce that the ISO's position in the organisation will be at management level, overseeing security orientated subordinates. This implies there is security awareness within the organisation and that the company is committed to the management of information security.

What is not implied by this appointment is to whom the ISO reports to in the organisation. You might expect the advert to mention "*reporting directly to senior management*" as do many other jobs, but this is not mentioned. This goes back to demonstrating an organisations overall commitment to security issues.

## Risk Management

We are taught that there are no absolutes in security. As users and managers of information people need to feel in control, and this is only available through appropriate risk management strategies.

According to a 2005 NHTCU report on *The Impact on UK Business 2005*<sup>8</sup>, states that 70 percent of the respondents believe that sufficient resources are being invested (in their organisation) to prevent computer-enabled crime. This, in my opinion, is unusually high given that if a threat agent wishes to launch an attack, or steal some information, it is unlikely that the measures in place will stop a really determined criminal. Of course, the ISO must at least appear convinced that the security measures in place are sufficient, otherwise the company would soon discover the weaknesses of the systems.

It is also fair to say that this complacency is not uncommon within UK businesses. As a nation we consider ourselves to be fairly technologically advanced. The same NHTCU report highlights that over half of IT staff employed in respondent companies have no formal security qualification. By implication this suggests that the results from the original question, regards investment into sufficient resources, could be ambiguous due to the insufficient skills of the respondents to analyse their security and information system.

Despite an organisation's poor ability to assess the effectiveness of their security system, organisations still need to implement risk management, which is the process that manages *risk assessment* and *risk control*.

Risk is the probability that a threat agent will exploit system vulnerabilities and thereby create an effect detrimental to the security system<sup>9</sup>. "Detrimental" in this case refers to anything that will make the system behave differently, or behave in an abnormal manner.

As a management process, Risk Management is designed to establish and maintain an Information Security System (ISS). There are several distinct approaches:

- quantitative – based on probabilities
- qualitative – based on expert knowledge
- knowledge-based – reuse best practice techniques
- model-based – object-orientated (all stake-holders involved)

It is the responsibility of the ISO to determine the specific approach to take but in my opinion this can only be applied after understanding the initial business process.

The first key step within risk management is the concept of risk assessment. Risk assessment starts by analysing the business first, so understanding the supply chain is essential to creating a successful assessment. It was discussed during the Security Management module that:

*“The ISO is responsible and inherently accountable for gathering and assessing information related to the organisations operations that can adversely affect the security and subsequently the profitability of the organisation.”*

If the ISO fails to understand the requirements of the business, there is a danger that numerous risks will not have been accounted for. It will then be obvious to the management that the ISO has failed his duties and therefore directly accountable for the security incident.

### **Threat Analysis**

Unconsciously, on a daily basis, we rectify attacks using our knowledge without really estimating the importance of our actions (most of the time)<sup>10</sup>.

The ISO will be required to guide the organisation in identifying:

- assets that require protection
- appropriate levels / methods of protection
- possible cost of implementing the protection

As a result, risk assessment must produce results that are meaningful and in which a high degree of confidence can be placed, implying therefore that qualified information needs to be entered into an assessment system so that the results are meaningful. A good way of testing a risk assessment strategy is to run the process again, and if the results are the same, then there is a high probability that the assessment is valid.

The ISO's job with regard to threat analysis is to determine as many weak links as possible. If the threats are not easily contained through expenditure on hardware or policies, the ISO should educate the relevant departments, making them aware of the possible threats and consequences.

Threat analysis is a comprehensive area within information security. The ISO must be aware of the varying threats that could effect the operation of the business. This will range from simple 'internal employee' threats to more complicated and more difficult to predict, 'environmental' threats (sometimes known as "acts of God").

Social Engineering is an often unrecognised threat even though it is a common method for obtaining access or by-passing security. Many employees are completely unaware that they're the *weak link* in an organisations control of information.

Often, front-line staff (who talk directly to the public) are the target of social engineering. They provide the easiest route to a good social engineer obtaining the information they

require. Kevin Mitnick's autobiographical book "*The Art of Deception*"<sup>11</sup> contains many examples of social engineering cases, for instance,

*When Mary picked up the phone, I told her my little story about computer problems, which was designed to give her the jitters so she'd be glad to cooperate. As soon as I had talked her through changing her password, I then quickly logged onto the system with the same temporary password I had asked her to use, test123.*

He also goes on to say:

*The lethal combination is when you exploit both people and technology...*

*...what I found personally to be true was that it's easier to manipulate people rather than technology*

After reading various social engineering cases I tried to locate some useful statistics. Not only could I find no statistics, I discovered another excerpt from an article that Mitnick wrote describing how businesses were not too forthcoming with information about social engineering attacks. The reason for little social engineering statistics is mostly out of pride, and that the examination of such incidents could be quite harming to the businesses reputation.

## Development of Policies

After understanding the risks and threats, an ISO will be more aware of what to allow and what not to allow within an organisation. This can be formally written to form the company security policy, providing a framework for best operational practice.

Usually, an Information Security Officer would create a security policy for the organisation. If it does not exist, it is the ISO's duty to construct such a document to protect the company's assets. The security policy is usually constructed from several other policies such as the privacy policy, access policy and the network policy. These separate policies constitute the sections within the main security policy.

If the policy does not exist, the ISO has many sources for generating a policy, a few of which are listed below:

- SANS Institute provides resources on policy<sup>12</sup>
- Request for Comments – specifically RFC2196<sup>13</sup>
- Other organisations (such as Universities)

When using another policy as a guideline, the ISO must be aware that different organisations are going to have different requirements. An educational establishment for example is required to provide access to hundreds if not thousands of new users each year. This will have an impact on the rules you can apply to the users of the network.

The SANS Institute<sup>14</sup> provides numerous templates for helping organisations develop a successful policy collection. As a rule, SANS have developed a basic framework for any policy containing the following sections:

1. Overview of the policy
2. Purpose of implementing such a policy
3. Scope of the policy
4. Policy detail
5. Enforcement of the policy (disciplinary action)
6. Definitions of any terminologies used
7. Revision history of the policy (who modified what and when)

One of the main considerations when implementing policies is to remember that as the business evolves, the policy will too. This means that the management and updating of policies requires review every 6-12 months. This will ensure the policies contain the latest business assets.

### **Standards & Models**

A core requirement of the information security officer is the goal of making the organisation either ISO17799 or BS7799 certified (ISO in this phrase stands for International Standards Organisation). Certification comes at a cost, and lasts for three years, but the advantages of being certified mean that the organisation can do business with other certified companies. The organisations can then be assured that both meet strict security guidelines.

One advantage of being certified is that to comply with the standard, the ISO must examine the business in terms of its position in the supply chain. This, if not already covered by the security policy, will be of great help when developing a contingency plan for the organisation.

The ISO should also be capable of deciding how much information can be given to certain parties and other organisations. This form of compartmentalisation provides information to users on a 'need to know' basis which, as good as it sounds, can create more problems by introducing issues with inter-office communication.

The ISO is given several security models to choose from, including "need to know" which is one of the oldest forms of information management. Although each specific model has its own advantages and disadvantages, a common practice is to create a combination of the different models, extracting the best (or most relevant) sections from each. The reason for selecting different sections from several models is that they all originated from different industries, for instance, military, educational or software engineering.

The CIA model is a simple model that has been developed from a need for standardisation, based on authorisation. Its three main sections are:

1. confidentiality: protecting information from unauthorised access and disclosure
2. integrity: safeguarding the accuracy and completeness of information and processing methods
3. availability: ensuring that information and services are available to authorised users

The second of the two models is DDPRR which is made up of the following five sections:

1. deter – create and implement a feasible deterrence
2. detect – when / where an intrusion took place
3. protect – create and implement policies
4. react – what to do when it happens
5. recover – what to do afterwards

Depending on the structure of the organisation, the ISO will be required to apply a model in order to assess the risks.

## The Laws

It is the ISO's responsibility to make sure that what is stated in the security policy complies with the UK's computer legislation. An information security officer should be aware of the following main computer Laws governing the day to day legalities of any organisation:

1. CMA – Computer Misuse Act 1990<sup>15</sup>
2. RIPA – Regulation of Investigative Powers Act 2000<sup>16</sup>
3. ECA – Electronics Communications Act 2000<sup>17</sup>

The Computer Misuse Act (CMA) was created in 1990 with the primary goal to plug loop-holes in legislation to include computer crime (mainly unauthorised access to systems).

The main criticism of this Act is that it is claimed to have been diluted in Parliament and that it only progressed it as far as a Private Members bill.

The Act does not define what a 'computer' actually is, which allows for future-proofing, as this now covers such devices as PDA's, mobile smart telephones. Although this may appear as a clever omission, it does leave the concept of a computer open to debate by non-technical jury's.

It contains three main sections:

1. unauthorized access
2. unauthorized access with the intent to commit further offences
3. unauthorized modification

The Regulation of Investigation Powers Act (RIPA) ensures that the investigatory powers are used in accordance with human rights.

1. interception of communication
2. intrusive surveillance
3. covert surveillance

The main point of this act is to specify that you cannot monitor or intercept communications without consent, unless you are:

1. the system administrator of a network
2. the owner of the system gives you authorisation

The Electronic Communications Act (ECA) introduced in 2000 is designed to build confidence in electronic commerce. It started development in 1997 taking three years to be fully introduced.

It too is made up of three key sections:

1. cryptography service providers
2. facilitation of electronic commerce
3. miscellaneous and supplemental elements

## Incident Management

Incident response is a disciplined approach to handling security breaches. The ISO should be informed of all security incidents as this may have an impact on the security policy (and therefore the life cycle of the policy).

Generally the following entities should be involved in handling an incident:

- Executive staff
- Human resources
- Physical security
- Law enforcement
- Public relations
- Directors / stake holders
- Business units / first point of contact
- Information Security Officer

Each has their own key role in handling an incident, for instance, the public relations office may be required to release a press statement after an incident.

The ISO needs to be proactive in planning and preparedness, for the eventuality that an incident will occur. The main key steps for managing an incident include:

1. Protect evidence and activity logs to create an audit trail
2. Containment of the incident (if it is a computer issue, possibly disconnect the machine from the network)
3. How serious is the incident? The ISO must be able to identify the severity of the incident, alerting the necessary entities (above).
4. Complying with regulations
5. Obligation to prevent misuse of company equipment

The Site Security Handbook <sup>[13]</sup> (formally known as RFC 2196) has an interesting point regards incident management stating that:

*One of the most important, but often overlooked, benefits for efficient incident handling is an economic one. Having both technical and managerial personnel respond to an incident requires considerable resources. If trained to handle incidents efficiently, less staff time is required when one occurs.*

Of course, this is dependant on the size of the organisation. If the company is small, it is likely that the security officer has a primary job function other than security, so an incident would involve dropping any 'normal' work to deal with the incident.

### **Awareness and self learning**

Amongst the monotonous tasks of creating and maintaining security policies, a security officer should be continually learning and evolving their techniques.

One of the easiest ways of obtaining the latest security information is to share knowledge with other organisations of a similar organisational structure. If one organisation has been affected by a particular type of security threat, it is highly likely that the same threat will be performed against the other.

Other learning strategies include subscribing to computer security magazines such SC Magazine, or simply to subscribe to security related news groups.

## ***Application to Business***

Most businesses will understand computer security from the concepts outlined in the 'history' section of this report. They believe that security consists of a few firewalls and typically some virus protection for the mail. Threats and the increase in threat agents have outgrown those simple defences and in some cases the cost has outgrown the approval level of expenditure which an ISO can endorse.

As a result, the ISO is now required to 'justify' his position, expense and activities through means of Return On Investment (ROI) to board level management. This leaves the ISO with three major problems<sup>18</sup>:

1. to build a business case that non-technical staff and management will understand and support
2. to determine the appropriate level of security for the company
3. to show that there is a financial return resulting from the investment

This, of course, will prove very difficult to achieve as the system implemented is non-profit making, and if working correctly, does nothing.

Justifying the expense of implementing security is a core function of the ISO job. Explaining security concepts to senior executives is a challenge, but as a recent article in Security Advisor Middle East<sup>7</sup> on *Return On Investment* discusses, mental pictures and diagrams work well. Their suggestion is to use a castle-and-moat analogy, for example:

*Explain that you're building a moat around a castle. Until you get the moat completely around the castle, you've spent a lot of money with no improvement in security.*

*Until you've established a minimum level of protection, you're spending a lot of money but are still totally vulnerable.*

The analogy goes on to explain how digging a shallow moat and having it a mile wide is a waste of money. You would be spending a great deal of money and not getting any results in return. This is like a form of business insurance; it is necessary to spend money to insure against losses of material, fire or flood, or personal injury - everyone hopes it will never happen, but when it does the insurance policy offers some ability to offset the loss. The ISO cannot guarantee absolute protection, only minimising the damage, however, to get to this position requires expenditure by the organisation.

Despite the inherent difficulties in justifying expenditure on security measures, the ISO still needs to evaluate dependencies within organisation and look at the position of the business within the global 'supply chain'. Finding the weakness in a supply chain will help the organisation develop contingency plans if that link was to fail.

## Conclusions

My initial question regards the roles and a responsibility of an ISO was to ask whether we actually needed one? Subsequently from writing this report I have convinced myself that the job of an ISO is unquestionably essential. I believe the difficulty will be in convincing an organisation with no security practices, that they will require somebody with the skill-set outlined during this report.

Most companies understand the requirements to have locks on doors, computers with passwords, but often forget (or choose to ignore) the requirements to use the skills of an ISO or the experience they offer. According to the Scotland Yard Computer Crime Unit<sup>19</sup>, employers are:

- Failing to address the company's own security issues
- Not making staff aware of the policies in place
- Not ensuring that employees have signed up to the policy
- Failing to remind staff regularly what is acceptable and what is not
- Offering no warning to staff of the dangers of being conned by hackers into giving away access information (refer back to social engineering).

My main criticism of security roles advertised in the press is that they ask for certain qualifications and skill-sets that would not normally be found together. For example, where the ideal candidate could implement a series of practices such as BS7799 Auditing, be CCSE Qualified and have an MSc Information Security with 4 years experience in an ISO based management role.

I believe this is due to a lack of understanding about certifications and standards from the management staff, and as a result the applicants for such jobs are only going to have a subset of the required practices.

As previously stated, the ISO's position within the organisation is often an indicator of the commitment of the management towards security within the business. The higher the security officer in the hierarchy, the greater the liaison will be with the business management structure and it is likely that the company will place a higher value on its security.

An overall increase in security threats and the increase in home computers being Internet enabled, means the ISO's job should be safe for a few years. This is sadly due to the recent terrorist attacks on the USA, and more recently the London bombings. A now outdated journal written by Leslie D Ball<sup>20</sup> examines the effect the terrorist attacks have had on the information security officer's role. The journal explains that as well as managing all of the responsibilities that have been outlined in this report, the security officer must now plan for potential terrorist attacks. This is an obvious step-up from the usual incident management policies.

In summary, an ISO's job is to manage the flow of information entering and leaving an organisation to minimise loss or damage. This is obviously going to be a mammoth task but with support from management and key departments like IT, it should be possible to implement a successful information security policy.

After implementing the policies, it is then the responsibility of the ISO to maintain and enforce the rules outlined, educating users of the implications of the actions they take.

## Background Reading

### **White Papers & Reports**

ASIS Online (2004) *Chief Security Officer (CSO) Guideline*  
BarclaySimpson (2005) *Information Security Market Report 2005*  
CIO (2005) *Incident Response: Response & Reporting Guidelines*  
Computer Security Institute (2005) *CSI/FBI Computer Crime and Security Survey*  
Control Data (1999) *Why Security Policies Fail*  
Kroll (2004) *Protecting Corporate Secrets*

### **Websites**

Essex Police (2005) *About Us: Information Security* [Online] Available From:  
[http://www.essex.police.uk/about/a\\_dp\\_10.php](http://www.essex.police.uk/about/a_dp_10.php) [Accessed 10th Oct 2005].

WGBH educational foundation (2003) *The Laws: Computer Fraud and Abuse Act*  
[Online] Available From:  
<http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html>  
[Accessed 14th October 2005]

Hal Abelson (1999) *Readings on Computer Crime* [Online] MIT Available From:  
<http://www.swisbs.ai.mit.edu/6805/readings-crime.html> [Accessed 14th October]

CSO Online (2005) *The Resource for Security Executives* [Online] CXO Media Inc  
Available From: <http://www.csoonline.com> [Accessed 14<sup>th</sup> October 2005]

Information Security Policy World (2005) *Security Policies* [Online] ISPSG, Available  
From: <http://www.information-security-policies-and-standards.com> [Accessed 15<sup>th</sup>  
October 2005]

SuperhighwaySafety (2001) *Computer Misuse Act 1990* [Online] Crown copyright -  
DfES and Becta, Available From:  
<http://safety.ngfl.gov.uk/ukonline/document.php3?D=d10> [Accessed 15<sup>th</sup> October 2005]

Dolan, A., (2001) *SANS Social Engineering Papers* [Online] SANS Institute, Available  
From: <http://www.sans.org/rr/whitepapers/engineering/> [Accessed 30<sup>th</sup> October]

### **Magazines**

SC Magazine August (2005), Article: Policy Management  
SC Magazine October (2005), Article: Risk Opinion

***Journals***

Ball, Leslie D.. *Information Systems Security*, May/Jun2002, Vol. 11 Issue 2, p25, 5p; (AN 6622961)

Tiller, Jim. *Information Systems Security*, Nov/Dec2003, Vol. 12 Issue 5, p2, 3p; (AN 11125482)

## References

- <sup>1</sup> Blyth, A. and Kovacich, G. L., (2001) *Information Assurance: Surviving in the Information Environment* [Book] Chapter 7 – The Corporate Security Officer [Page 109]
- <sup>2</sup> Deloitte (2004) *Global Security Survey* [Online] Deloitte Touche Tohmatsu. Available from: <http://www.deloitte.com/dtt/research/> [Accessed 14<sup>th</sup> Oct 2005].
- <sup>3</sup> ASIS Online (2004) *Chief Security Officer Guidelines* [Online] ASIS International. Available from: <http://www.asisonline.org/guidelines/guidelineschief.pdf> [Accessed 11<sup>th</sup> Oct 2005].
- <sup>4</sup> Unknown (Unknown) *The Robert Morris Internet Worm* [Online] Available From: <http://www.swiss.ai.mit.edu/6805/articles/morris-worm.html> [Accessed 13th Oct 2005]
- <sup>5</sup> Unknown (2005) *Article On Security* [Magazine] Computing, October Issue 13 [Page 10]
- <sup>6</sup> SC Magazine (2005) *Classified Adverts: Job Section - BarclaySimpson* [Magazine & Online] Haymarket Publications, August [Page 85] Available From: <http://www.barclaysimpson.com> [Accessed 11<sup>th</sup> Oct 2005]
- <sup>7</sup> Unknown (2005) *The State of Information Security 2005* [Online] CIO Magazine. Available From: <http://www.csoonline.com/csoresearch/report93.html> [Accessed 20th October 2005]
- <sup>8</sup> Unknown (2005) *The Impact On UK Business 2005* [Online] NHTCU Available From: [http://www.nhtcu.org/media/documents/publications/8817\\_Survey.pdf](http://www.nhtcu.org/media/documents/publications/8817_Survey.pdf) [Accessed 21st Oct 2005]
- <sup>9</sup> Vidalis, S., (2005) *Threat Assessment Lecture* [Lecture Notes] University of Glamorgan
- <sup>10</sup> Dr. Stilianos Vidalis (2005) *Security Through Deception* [Lecture Slides] Pro-Logos [3<sup>rd</sup> Slide]
- <sup>11</sup> Kevin Mitnick (2003) *The Art of Deception* [Book] Wiley. Chapter 8 [Page 119]
- <sup>12</sup> Unkown (2005) *SANS Policy Project* [Online] SANS Institute. Available From: <http://www.sans.org/resources/policies/> [Accessed 30<sup>th</sup> Oct 2005]
- <sup>13</sup> Fraser, B., (1997) *RFC 2196 – Site Security Handbook* [Online] NWG. Available From: <http://www.faqs.org/rfcs/rfc2196.html> [Accessed: 31 October 2005]

- 
- <sup>14</sup> Unknown, (2004) *The SANS Security Policy Project* [Online] SANS Institute. Available From: <http://www.sans.org/resources/policies/#template> [Accessed 15<sup>th</sup> Oct 2005]
- <sup>15</sup> Unknown (1990) *The Computer Misuse Act 1990* [Online] Crown Copyright. Available From: [http://www.opsi.gov.uk/acts/acts1990/Ukpga\\_19900018\\_en\\_1.htm](http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm) [Accessed 15<sup>th</sup> Oct 2005]
- <sup>16</sup> Unknown (2000) Regulation of Investigatory Powers Act 2000 [Online] Crown Copyright. Available From: <http://www.opsi.gov.uk/acts/acts2000/20000023.htm> [Accessed 15<sup>th</sup> Oct 2005]
- <sup>17</sup> Unknown (2000) Electronic Communications Act 2000 [Online] Crown Copyright. Available From: <http://www.opsi.gov.uk/acts/acts2000/20000007.htm> [Accessed 15<sup>th</sup> Oct 2005]
- <sup>18</sup> Unknown (2004) *Selling Security to the Board* [E-Magazine] Security Advisor Middle East, Issue 8 [Accessed 11<sup>th</sup> Oct 2005]
- <sup>19</sup> Bill Goodwin (2003) *Companies' poor security policies hamper police investigations into computer crime* [Online] Computer Weekly. Available From: <http://www.computerweekly.com/Articles/2003/08/05/196400/Companies'poorsecuritypolicieshamperpoliceinvestigationsintocomputercrime.htm> [Accessed 17<sup>th</sup> Oct 2005]
- <sup>20</sup> Ball, Leslie D.. Information Systems Security, May/Jun2002, Vol. 11 Issue 2, p25, 5p; (AN 6622961)