THE ORGANISATIONAL INFORMATION SECURITY PROFILE

- A TOOL TO ASSIST THE BOARD –

Mkhululi Tyukala[1], Dalenca Pottas[2], Helen van de Haar[3], Rossouw von Solms[4]

Nelson Mandela Metropolitan University, Port Elizabeth, South Africa

[1]mkhululi.tyukala@nmmu.ac.za [2]dalenca.pottas@nmmu.ac.za [3]helen.vandehaar@nmmu.ac.za
[4]rossouw.vonsolms@nmmu.ac.za

ABSTRACT

What does the senior management of an organisation do when the board of directors asks, "show us that the organisation's information security policy is implemented and maintained properly"? Such a question is likely to be asked as part of the board's effort to show that it has met its obligations in terms of due diligence. This paper introduces a framework to facilitate the governing of information security in an organisation. The framework defines the concept of an organisational information security profile (OISP), the role of which is to retain and measure the level of efficiency of information security and inform the board accordingly.

The paper discusses the OISP and each of its major building blocks. Each building block and its role are explained in detail. Ultimately the OISP will show how the information security of an organisation has been implemented based on the information security policy of the organisation and the changes that have taken place over time, therefore pointing out areas that need immediate attention.

KEYWORDS

Organisational information security profile, information security program, information security requirements, controls, control Attributes

THE ORGANISATIONAL INFORMATION SECURITY PROFILE

- A TOOL TO ASSIST THE BOARD -

1 INTRODUCTION

Information is the glue that holds an organisation together (Eloff, Labuschagne, & Badenhorst, 1993). Compromise to its confidentiality, accuracy and timeliness may lead to huge financial losses and result into a negative impact on the image of an organisation (Posthumus & Solms, 2004). In order to prevent loss of information and subsequent damage to the organisation, it is imperative that information is secure at all times.

However, due to its complexity and the variety of issues it encompasses, information security has always been treated as a technical issue that could be managed with technology only. According to Conner et al, information security was treated like this due to the lack of frameworks of action on how to set priorities, assign tasks, get started, and monitor implementation. That is, there was no recognized, standard approach at an organization-wide level to help determine what should be done and who should do it.

To ensure that information security is taken serious throughout the organisation, the last few years have seen information security being elevated to board of director level. New legislations, such as the ETC Act (ECT ACT, 2002), King Report (King II Report, 2001), Sarbanes - Oxley Act of 2002, and Health Insurance Privacy and Accountability Act (HIPAA) of 1996 (Conner et al., 2004), are the driving force behind the elevation of information security to the board level. Etsebeth and Von Solms also echo this: "organisations are being placed under increased pressure by means of new laws, regulations and standards, to ensure that adequate information security exists within the organisation" (Etsebeth & von Solms, 2004).

Effective security of information is achieved through the combined efforts of responsible information systems owners, users, custodians, security personnel, customers, and other stakeholders (Conner & Swindle, 2004). However, the board of directors and executive management play a far more significant role in the success of the information security endeavours of an organisation. The executive management of the organisation is responsible for the implementation of information security and the board of directors is accountable, as part of its duty care, to provide effective information security oversight (Le Grand, Parker, & Thomas, 2001), (von Solms & von Solms, 2004a), (Parker, 2001). However, the involvement of the board of directors in information security is mostly through periodic briefings from executive management on the well-being of the organisation.

A survey conducted by Ernst & Young, found that the board is only briefed via periodic reports on what has been implemented or on the status of information security (Ernst & Young, 2003). The briefings are done to see if the information security program of the organization is effective or not. Effectiveness or ineffectiveness of the information security program is a measuring stick on how secure the information and information systems of an organization are. However, of the more than 1400 organisations (from 66 countries) that were sampled in the afore-mentioned survey, only 6% actually report to the board on a continuous basis.

There is no documented system, known to the authors, which brings together under one cover all the requirements of an effective information security program mentioned above. That is, accommodate the needs of the board of directors, executive management and information security specialists at the lower levels of the organisation.

In that regard, the objective of this paper is to introduce a mechanism called the organizational information security profile (OISP). This OISP will be built to accommodate the needs of the board of directors at the top as well as the information security managers at the lower levels of the organisation. The framework will assist in building, determining and maintaining the effectiveness of the security program, therefore pointing out if the security program is in line with the vision of board of directors or not.

This paper will firstly address the issue of defining an OISP in Section 2. This will include a presentation of what is needed to build an OISP, with each building block discussed in Sections 3, 4 and 5. Secondly, information security incidents and their effect on the OISP will be high-lighted in Section 6. Information security incidents are expounded on in their capacity of affecting the effectiveness of the information security program. Thirdly, a detailed presentation on how to build an OISP will be provided in Section 7. It will be argued that an organization can maintain an acceptable level of security for their assets in spite of information security incidents. The paper will conclude by providing an overview of how the OISP can be used to determine the status of the information security in the organization.

2 THE ORGANISATIONAL INFORMATION SECURITY PROFILE (OISP)

The OISP will be based on the security profile as defined by Whitman and Mattord (Whitman & Mattord, 2005): That is, "a security profile or security posture is representative of the implementation of security in an organization" (Whitman & Mattord, 2005). It can be argued that a security profile is a mechanism by which an organisation could get a complete overview of its information security program. This characteristic of the security profile will be a fundamental requirement of the OISP. An overview of an organisation’s security posture will accommodate the needs of all role players insofar as information security is concerned.

Additionally, the requirement for a complete overview of the information security program is motivated by the information security needs of the board of directors. The information security needs of the board of directors, stated simply, are: the things the board must know so that they can provide oversight of information security. According to Le Grand, the essential function of the board of directors towards information security is to ask the right questions about information security to the executive management (Le Grand, 2000). The goal of the questions is to seek assurance from executive management that information security is implemented according to the organisation's information security policy. The questions that the board should ask, include (Le Grand et al., 2001):

(a) The greatest technology risks that the organisation is facing and what measures have been put in place to mitigate them.
(b) Whether the resources provided for information security are sufficient.
(c) If information security is properly managed.

These questions (or information security needs of the board of directors) further highlight a need for the above-mentioned mechanism (OISP) to provide a snapshot of an organisation's information security. An information security snapshot means: At any given time, an organisation should be able to obtain the areas of concern from its information security program and evidence why the problems exist. This could be due to new threats that were not part of the initial security program. To show how the OISP would answer the questions of the board of directors and other role players, it is imperative that the conceptual foundations of the OISP are thoroughly presented.

2.1 Conceptual Foundations of the OISP

To support the questions (or needs) of the board of directors, it is imperative that the OISP provides an organisation with the following abilities: initialisation (or modification), monitoring, measuring or reviewing, and reporting on the information security program. This is a cyclic process.

After initialization (or modification) of the information security program; organisations need to monitor information security so that acceptable levels are maintained. Furthermore, the effectiveness of information security needs to be measured. Measuring will provide organisations with the knowledge whether information security is effective or not. In the end, the effectiveness of information security needs to be reported to appropriate parties, such as the board of directors. This will ensure that the necessary changes can be made to maintain the effectiveness of information security. Any change to the organisation requires support from the board of directors. With the support of the board, security managers can get all the financial backing they require to maintain the effectiveness of the information security program.

To show how the OISP will support the information security needs of the board of directors, it is imperative that a definition of the OISP and its characteristics are provided. The definition will provide a common foundation and understanding of an OISP.

Definition (Organisational Information Security Profile): an entity which is representative of the implementation of the information security of an organisation and possesses the ability to:

(a) Enable the information security program to adapt to the changing business environment and technology. Organisations change their business environment by changing the business strategies to adapt to the changing market so that they remain competitive. The OISP will also need to adapt to the changing technology in the organisation. Technology changes rapidly. Therefore, organisations should respond to the change to take advantage of the benefits of better and more effective and efficient technology. Introduction of new technology will affect the level of security. Changing the business strategy or technology opens doors to new risks. New risks might cause harm to the organisation because the organisation did not implement measures, initially, to protect itself from them.

(b) Provide a snapshot of the information security program at any given moment. This will make it straightforward for the executive management to brief the board of directors about the effectiveness of information security should the need arise. Through the OISP, the organisation would be able to point out the changes in the information security program at any given time.

(c) Provide the status of information security. The status would be a reflection of the ability of the individual components of the information security program to keep the organisation safe from harm.

(d) Enable the security program to be extended (i.e. more features can be added to it) in order to maintain the effectiveness of security controls. The OISP should provide an organization with a holistic view of its information security. It follows that the OISP will help the organisation to point out areas that need to be strengthened. Ultimately, the OISP should be able to provide evidence about the problematic areas. That is, the cause of the problematic areas.

(e) Reflect change over a period of time. That is, organisations may take a snapshot of the information security program and from its status they may identify a need to improve certain areas. However, it is imperative that the organisation be able to see how (and whether) the measures implemented to address problem areas, improved security.

Finally, the OISP will acquire the above-mentioned abilities through what is referred to as the building blocks of the OISP. The building blocks are security requirements, information security controls and control attributes. The next three sections discuss the three building blocks of the OISP.

3 INFORMATION SECURITY REQUIREMENTS

Information security requirements outline the qualities of information assets that are important to an organization (Alberts & Dorofee, 2001). That is, information security requirements dictate the degree of confidentiality, integrity and availability (CIA) that must be put in place for information and IT systems (Gerber & von Solms, 2001).

According to the Software Productivity Consortium, information security requirements are based on the information security policy, regulations, laws, and functional (business) requirements of an organisation (Software Productivity Consortium, 2004).

Furthermore, ISO17799 states that information security requirements can be determined from three sources, namely (ISO17799, 2000):

(a) from assessing risks to the IT infrastructure of the organization,
(b) legal, statutory, regulatory and contractual requirements that an organisation and its trading partners, contractors and service providers have to satisfy and
(c) a set of principles, objectives and requirements for information processing that an organisation has developed to support its operations.

3.1 Identifying Information Security Requirements

According to Gerber and von Solms, information security requirements are determined by a process called Security Requirements Analysis (SRA) (Gerber, von Solms, & Overbeek, 2001). They state that SRA is initiated by asking questions to role players responsible for security and those responsible for information in the organisation.

The questions are divided into two categories. That is, business related questions and loss impact related questions. Business related questions, relate to all the questions concerning the level of confidentiality, integrity, availability, auditability and authenticity that an organisation requires for its assets (Gerber et al., 2001). The level of each concern can be high, medium, low or none. Gerber states that business questions are usually a list of multiple-choice questions about each of the five concerns.

Impact related questions, relate to all the questions concerning the business harm that could result if the security of the individual assets is compromised. Roy et al defines the loss impact as the monetary estimate or some other intangible impact such as loss of customer confidence, competitive advantage or the organisation's reputation (Roy, Barik, Mazumdar, Dastidar, & Sengupta, 2004). In addition, loss impact can be fines, legal penalties, financial, or productivity. The level of loss impact can be high, medium, low or none.

The level of security of each asset of the organisation can be determined by combining the five security concerns levels and loss impact levels in the following manner:

Information Asset = (confidentiality, loss impact) + (integrity, loss impact) + (availability, loss impact) + (auditability, loss impact) + authenticity, loss impact). Each concern and impact level combination will result into 16 possibilities. Therefore, each asset will have eighty (16 x 5) possibilities. However, some of the concern and impact level possibilities would result in a level equalling none.

Using appropriate values for the security concerns and the loss impact, an organisation can determine the numeric amount of security it requires for individual controls. For instance, if an organisation uses a scale of zero to five for security such that none = zero, low = (zero, 3), medium = [3, 5) and high = [5], then adding the values for each combination will give the numeric level of security for an asset. A thorough presentation of determining security levels can be obtained from (Gerber & von Solms, 2001).

The amount of security needed for an asset can then be scaled back to none, low, medium or high. Meaning, an asset can require no security, low security, medium security or high security. The

crux of the information security requirements approach is that organizations will implement information security by focusing on individual assets and security risks but end up with security that is uniform at all levels.

Information security requirements would enable any organization to determine its information security needs and levels. That is, information security requirements will enable an organization to initialize the information security program. Additionally, information security requirements would accommodate the geography, industry, budget, acceptable amount of risk, and size of any organization. Ultimately, information security requirements would enable an organisation to move from one security level to another, since each asset has a known level of security. An organization can decide to increase or decrease the amount of security to a higher or lower level to cater for the business strategy of that time.

Finally, after the information security program has been initialized and security requirements have been determined, an organisation would select information security controls to put in place to secure its assets. This leads to a discussion of the second building block of the OISP.

4 INFORMATION SECURITY CONTROLS

Information security controls are practices, procedures, or mechanisms that reduce security risks (Rees et al., 2003). Van de Haar and von Solms state that information security controls help organisations by providing the level of security organisation require for their information (van de Haar & von Solms, 2003). In other words, information security controls ensure that all the operations of the organization that require timely and accurate information can be continued without interruptions.

The role of information security controls in the OISP complements security requirements as presented in the previous section, that is, to secure the information and information systems of an organization based on the needs and levels of risk of the organisation. In other words, the security controls an organization implements for its information and IT systems is a reflection of the level of risk it is willing to accept. Additionally, ISO17799 suggests that to ensure their effectiveness, security controls must be determined at the security requirements stage.

However, after security requirements are determined and security controls put in place, there is no guarantee that they will remain effective and efficient. This is due to the changing business environment and technology under which security controls operate. Furthermore, information security controls only reduce known security risks to acceptable levels. Therefore, a changed business environment or technology may affect the effectiveness of security controls as old risks may have changed in nature and new risks may have emerged.

Therefore, there must be a mechanism by which information security controls can adjust to the changes in the business environment and technology. The next section will present control attributes - control attributes provide security controls with the ability to adjust to changes.

5 CONTROL ATTRIBUTES

Information security control attributes were first suggested by van de Haar and von Solms to help put in place effective information security controls in an organisation (van de Haar & von Solms, 2003). That is, to help ensure that information security controls remain effective when the organisation changes strategies or technologies. To help provide a clearer understanding of control attributes, a definition will be provided.

Definition (Control Attributes): Control attributes can be defined as all the processes or technologies that are put in place to make sure that an information security control functions effectively and efficiently in the organisation. Towards providing an example of control attributes, consider that a security control, say the data backup control, must have owner, incident

documentation, backup media from a reliable manufacturer, separation of duties and other control attributes.

Control attributes are driven by the information security requirements of an organisation. If an organisation requires a high, medium or low security level for a certain asset, then it will be possible to implement information security control(s) with control attributes to achieve that security level. Furthermore, the identification of control attributes for a security control will depend on the nature of the control, which in turn will depend on the individual organisation and its information security requirements. Each security control, for example technical controls and legal controls, may need a specialist for the selection of adequate control attributes. The use of control attributes will make it possible to 'measure' the level of security in the organisation.

The initial level of security of a security control will be a function of the control attributes that are implemented at the time when the security control is put in place. At a later point, there will be different control attributes in place. These changes can be measured over time and should indicate whether information security is in line with the business objectives and the vision of the board of directors as business boundaries change over time.

In concluding the building blocks of the OISP, by using information security requirements, information security controls and controls attributes it becomes feasible to audit individual security controls and also solve their problems without having to look at the entire OISP for answers.

Using the three building blocks as discussed previously, any organisation can build an OISP depending on the level of security it requires for individual assets. Furthermore, any organisation can build an OISP by:

(a) First determining the level of security it requires. This will be achieved through information security requirements.

(b) Secondly, putting in place security controls based on the level of security requirements.

(c) Finally, accompany security controls with control attributes. Controls attributes will ensure that security controls and therefore the information security program adapt to the changing nature of the business environment

However, using the OISP will not mean an end to information security challenges. Organisations will be faced with challenges from information security incidents. Information security incidents inadvertently provide a way to measure how effective the information security program of the organisation is. Consequently, the challenge of information security incidents motivates a presentation of information security incidents and their effect on the OISP.

6 INFORMATION SECURITY INCIDENTS

Information security incidents hereafter referred to as security incidents, have been prevalent as early as before the proliferation of the Internet and the World Wide Web (www). According to (Mather & Egan, 2005), in 1988 the Morris worm stopped 10% of all computers connected to the internet. This is of concern, considering the fact that currently organisations use the Internet as a vehicle to achieve business strategies and goals.

Hackers and terrorists use the Internet to spread their malicious activities. The activities include virus attacks, denial of service attacks and other related malicious activities. Furthermore, the last few years have seen a dramatic increase of security incidents. Between the years 2000 and 2003 security incidents were increasing 30 thousand security incidents per year (Cert Coordination Center, 2004).

This wide spread occurrence of security incidents motivates a look at what is a security incident? Moreover, what qualifies to be called a security incident?

Considering the purpose of this paper, the authors define an information security incident as:

Definition (information security incident): any activity conducted in the organisation that could result in loss or damage to organisation's assets, or a breach of the organisation's information security procedures, rules and regulations governing the use of information, information systems and services.

An example of a security incident in terms of the above definition, could be failure to update antivirus software, which may be required by the information security policy of the organisation. This type of incident differs from the lay person's view of an incident (such as a virus infection), in that it constitutes a violation of policy and may not have caused harm. Yet, it is considered to be a security incident, the occurrence of which must be stopped. Security incidents can be large or small scale in nature. Therefore, the level to which security incidents cause harm to an organisation will vary by situation and organisation. This leads to the following categorisation of security incidents.

6.1 Categories of Information Security Incidents

Security incidents help to point out if the effectiveness of an information security control is excellent, good, acceptable or bad in securing information and information systems. The level of effectiveness enables organisations to see whether a security control deters security incidents that may cause harm to the organisation. Therefore, the harm that an organisation can suffer is a function of the level of security of the individual security controls. Additionally, for any security incident that takes place in an organisation a number of possibilities come to life:

(a) First, a security incident takes place where there are countermeasures in place to offset it, and if the countermeasures are good enough the effect of the incident results into nothing.
(b) Secondly, an incident takes place but does not cause immediate damage to the organisation. However, if the security incident is left to continue a number of times, severe damage could be experienced by the organisation.
(c) Thirdly, a security incident takes place with countermeasures to offset it but it goes beyond them and causes havoc to the organisation. An example is an antivirus program but a virus still spreads around the organisation.
(d) Finally, a security incident takes place and causes harm to the organisation because there were no information security controls put in place to counter it. An example of such a security incident would be the recent tsunami.

The above (non-exhaustive) list of scenarios simply points out that a security incident can have varying levels of impact to the organisation. The severity of a security incident is a measure of the possible harm that it may cause to the organisation at a given moment. In line with the above-mentioned possibilities, a generic categorization is proposed for the severity of a security incident, namely:

(a) None (Category 1)
(b) Low (Category 2),
(c) Medium (Category 3), or
(d) High (Category 4).

The four possibilities will be referred to as the four impact categories of information security incidents. That is, Categories 1, 2, 3 and 4 respectively, as shown in brackets above and used in Table 1 (third column, second value in square brackets).

Note that this categorization does not propose a metric to measure the severity of a security incident, only the result of such a measurement. It should be kept in mind that although the severity of a security incident could be rated as "none", that does not mean that the security incident should be ignored. For instance, if users share their passwords, a once-off incident might not cause damage. However, if an organisation condones the sharing of passwords and one of the passwords falls into the hands of an unauthorised individual, that would be provoking security incidents. The unauthorised individual could gain access to critical organisational information. Ultimately, it

would be hard for the organisation to determine whether one of its authorised employees gained the access or not.

But how does the categorisation of security incidents play a role in the information security program? Within the context of this research, where the OISP serves as a mechanism to get an overview of the information security programme, it follows that the occurrence and categorisation of security incidents must be included in the OISP.

Table 1, as an example, represents two stages of an information security program. The first two columns, i.e. security control and control attributes, would be reflected in the OISP after the initiation of new information security program. An organisation initiates a new information security program by putting in place security controls to minimize risks to acceptable levels. The incidents column shows a later stage of the OISP, i.e. after security incidents have taken place. The incidents column reflects the number of times that an incident has taken place and the severity of the security incident over a (defined) period of time (although the period is not stated in this example). For instance, on the Information Backup control, there were two Category 2 incidents and one Category 3 incident.

Table 1: Example of an Organisation Information Security Profile

Security Control	**Control Attributes**	**Security Incidents** **[Frequency][Severity Type]**
Information Backup	Owner, Documentation of Incidents, Change Documentation, Staff IDs, Offsite Storage, Reliable Media,	Backup performed outside schedule [×2][2], Backup not done [×1][3],
Password	Minimum Length, Grace Period, Character categories, Incident Documentation, Password Lifetime , Maximum age, Minimum age,...	Forgot password [×10][2], Sharing violation [×2][2], Lifetime expired [×13][2], Grace Period expired [×5][2]
Physical Access Control (Entrance)	Owner, Documentation of Incidents, Staff Identification Cards, Visitor Identification Cards, Metal Detection	Staff forgot ID Card [×10][2], Visitor lost ID Card [×1][2], Staff refused detection[×1][2]
Anti-Virus Program	Incidents Documentation, Owner, Periodic Updates, Staff Training, Email Rules, OS Updates, Forbidden File Extensions, Periodic Audits, Alert service, periodic scans	Email attachment not scanned [×5][2], periodic scan not done [×2][2], forbidden file extension not filtered [×1][3], new virus detected [×1][4], virus not updated [×1][2]

For any organisation, the security incidents that take place will point out the areas that need attention in the OISP. The types of security incidents that took place and how they were handled will further determine how effective the OISP has been. This motivates the need to discuss how an organisation can determine the effectiveness of its OISP (or information security programme).

7 THE EFFECTIVENESS OF THE SECURITY PROGRAM

Before guidelines on how to determine the effectiveness of the information program are presented, it is imperative to highlight the importance of knowing the effectiveness of information security:

(a) An organisation may need to know the level of security after a change in business strategies. The level of security may also need to be determined after the updating of existing technologies or introduction of new technologies in the organisation.

(b) The board of directors needs to be kept abreast of the levels of security in the organisation. This information will inform the board of directors whether the assets of the organisation are secured or not. This is in line with their duty of care towards the well-being of the organisation. The effectiveness of security will enable an organisation to know if the level of security has remained the same, increased and decreased. Ultimately, determining the status of information security and updating the board of directors will make it possible to take new actions to maintain acceptable levels of security in the organisation.

The effectiveness of the overall information security program can be measured by examining the effectiveness of the individual security controls in the organisation. It will be reflected by the ability of the security control to counteract the information security incidents it is put in place for. Specifically, the effectiveness of each security control depends on:

(a) the severity of the security incident and
(b) the ratio of the number of incidents that were encountered against the number of incidents that the security control counteracted.

The ratio will further point out whether the effectiveness of a security control has changed since the first time it was put in place. Therefore, the current status of the security program can be determined by looking at the effectiveness of all the security controls in the OISP. Additionally, the current status of information security can be used to determine:

(a) if the information assets are secure enough,
(b) whether the level of protection offered by controls (and their associated control attributes) is increasing or decreasing, and
(b) if a security control has regressed to being a liability. A security control becomes a liability to the organisation if it does not succeed in its purpose of countering incidents and it requires more resources to be maintained than the value it adds in protecting assets.

Using the password control from the information security program above, suppose that the users forget their passwords every Monday or any other day. The help desk will be swamped by users needing new passwords, therefore affecting their daily duties. If the problem is left to continue it may affect the entire organisation in the long run. To solve the password problem an organisation may devise a password management awareness (or more general security awareness) programme to inter alia teach its users about the selection and management passwords.

Finally, Table 2 shows an example of the effectiveness of an information security program.

Table 2: The effectiveness of an information security program

Control Category	**Security Incidents**		**Managed Incidents**	**Damaged Caused**
	Security Control	**Total Incidents**		
Systems Security	Password	30	20	None
	Anti-Virus	10	7	5 PCs infected with viruses
	Data Backup	3	1	None
Physical Access Control	Entrance	12	0	None

Table 2 shows a selection of controls from the information security program arranged by control category. A control category is used in this example to illustrate that controls can be grouped to represent control areas (eg physical access control), which enhances the information for reporting purposes. However, this issue is not expanded on in this paper due to limits in scope.

The total incidents column is a measure of the number of incidents that took place per corresponding control. Managed incidents indicate the number of incidents that were resolved before they caused damage to the organisation. The damage caused column indicates the damage resulting from the incidents that were not handled successfully. For instance, the anti-virus control had a total of 10 incidents and 7 of them were resolved successfully. Meanwhile 3 of the incidents were not solved and therefore caused damage to the organisation.

The effectiveness of the entire information security program can be determined by looking at the number of managed incidents as well as the damage caused by the incidents. For instance, it is clear from Table 2 that the anti-virus control is ineffective due to the security incidents that were not managed and the damage that resulted from them.

An organisation can minimize security incidents and therefore improve information security by strengthening the security controls from which security incidents emanated. Security controls are strengthened by improving its set of controls attributes. The set of control attributes can be improved by adding more control attributes to the security control. For example, the password control listed in Table 1 can be strengthened by adding more control attributes such as education (on password security and management), enforcement of password history, minimum password length, complexity requirements, and the storage of passwords using reversible encryption.

Additional controls can be strengthened using the approach demonstrated above. The new security program resulting from the improved security controls is shown in Table 3.

Table 3: The OISP, with improved information security controls

Security Control	**Control Attributes**	**Incidents**
Information Backup	Owner, Documentation of Incidents, Separation of duties, Change Documentation, Staff Identification, Offsite Storage, Reliable Media, Monitoring, Daily Logs, Reporting	
Password	Minimum Length, Grace Period, Character categories, Incident Documentation, Password Lifetime, Maximum age, Minimum age, Minimum length, Passwords must meet complexity requirements, Store passwords using reversible encryption	
Physical Access Control (Entrance)	Owner, Documentation of Incidents, Staff Identification Cards, Visitor Identification Cards, Metal Detection, …	
Anti-Virus Program	incidents documentation, Owner, periodic updates, staff training, email rules, OS updates, forbidden file extensions, periodic audits, alert service, periodic scans	

Note that at this stage of the OISP, there are no recorded security incidents. This is because incidents will be recorded and measured against a revised, more effective set of controls and control attributes, once the first cycle of monitoring, reporting and modification has been completed.

Finally, the information contained in Table 2 can be presented to the board of directors when required. This can be done using a visually elucidating format which will assist the board to understand the information without including any technical and confusing details. The presentation will show the areas where incidents are being handled successfully as well as those that are problematic. The board of directors could be interested to identify areas that are experiencing more incidents and what measures need to be taken to stop similar incidents from happening again. Furthermore, the information gathered on the effectiveness of information security can be applied in

other enterprise risk management (ERM) processes to indicate which areas in the organisation carry more risk. The presentation to the board can further help the security managers get more financial backing for information security.

8 CONCLUSION

Elevating information security to the board of director level will provide organizations with far greater benefits than just legal or regulatory compliance. However, there is a lack of frameworks which accommodate the board at the highest organizational level as well as the technical people at the lower levels of the organisation. This paper showed how the organisational information security profile (OISP) can be used as a framework to govern information security in an organisation. This entailed the presentation of the building blocks of the OISP and the role each building block plays in the OISP.

The paper also explained how the effectiveness of the information security program can be determined using the building blocks of the OISP. Finally, the paper suggested that this information can be presented to the board of directors in the organisation without using the technical details of the OISP. Ultimately the OISP will show how the information security of an organisation has been implemented based on the information security policy of the organisation and the changes that have taken place over time, therefore pointing out areas that need immediate attention.

9 REFERENCES

Alberts, C., & Dorofee, A. (2001). An *Introduction to the OCTAVESM Method.* http://www.cert.org/octave/methodintro.html.

Cert Coordination Center, (2004). *CERT/CC Statistics 1988 – 2004.* http://www.cert.org/stats/.

Conner, B., Noonan, T., & Holleyman II, R. (2004*). Information Security Governance: Toward a Framework for Action*. (Business Software Alliance).

Eloff, J. H. P., Labuschagne, L., & Badenhorst, K. P. (1993). *A Comparative Framework for Risk Analysis Methods*. Computers & Security, 12 (6), 597—603.

Ernst & Young. (2003). *Global information Security Survey 2003*. http://www.ey.com/.

Etsebeth, V., & von Solms, B. (2004). *Legal Implications of Information Security Governance*. Unpublished Master's Thesis, University of Johannesburg. http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=125

Gerber, M., & von Solms, R. (2001). *From Risk Analysis to Security Requirements*. Computers & Security, 20 (7), 577 – 584.

Gerber, M., von Solms, R., & Overbeek, P. (2001). *Formalizing Information Security Requirements*. Information Management & Computer Security, 9 (1), 32 – 37.

ISO17799. (2000). *ISO 17799: 2000 Code of Practice for Information Security Management*.

Le Grand, C. (2000, February). *Responsible Internet Neighbors: Board Concerns for Information Security* (No. 3).

Le Grand, C., Parker, X., & Thomas, H. (2001, February). *Information Security Governance* (No. 4). http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=383

Mather, T., & Egan, M. (2005). *An Executive's Information Security Challenge*. Addison Wesley Professional.

Parker, X. (2001). *Information Security Governance - What the Board Needs to Know*. http://www.theiia.org/.

Posthumus, S., & Solms, R. von. (2004). *A Framework for the Governance of Information Security*. Computers & Security, 23 (8), 638 — 646.

Roy, J., Barik, M., Mazumdar, C., Dastidar, K. G., & Sengupta, A. (2004). *A Markup Language for Enterprise Security Requirements Specification*. http://cs.uiowa.edu/ kghoshda/XMLpaper.pdf.

Software Productivity Consortium. (2004). *Security in the Systems Development Lifecycle*. http://www.systemsandsoftware.org/security/papers.

Van de Haar, H., & von Solms, R. (2003, April). *Deriving Information Security Control Profiles for an Organization*. Computers & Security, 22 (3), 233 – 244.

Von Solms, R., & von Solms, B. (2004a, June). From Policies to Culture. Computers & Security, 23 (4), 275 – 279.

Whitman, M. E., & Mattord, H. J. (2005). *Principles of Information Security* (2 ed.). Thomson Course Technology.