Fourie, L. C.H.

Article

The management of information security: A South African case study

South African Journal of Business Management

Provided in Cooperation with:
University of Stellenbosch Business School (USB), Bellville, South Africa

Suggested Citation: Fourie, L. C.H. (2003) : The management of information security: A South African case study, South African Journal of Business Management, ISSN 2078-5976, African Online Scientific Information Systems (AOSIS), Cape Town, Vol. 34, Iss. 2, pp. 19-29, https://doi.org/10.4102/sajbm.v34i2.679

This Version is available at:
https://hdl.handle.net/10419/218280

The management of information security – A South African case study

L.C.H. Fourie
Graduate School of Business, University of Stellenbosch,
PO Box 610, Bellville 7535, Republic of South Africa
lchf@usb.sun.ac.za

Received May 2003

The growing misuse of information technology and the increased dependence on computer technology and systems heightened the requirements for information security. Unfortunately there often is a feeling of apathy towards information security by management, which leads to an ad hoc approach to information security and resultant information and financial losses.

The main objective of the research thus was to determine the current state of information security at a large manufacturing company in South Africa. The methodology entailed a field study of which three sets of structured questionnaires on information security were an important component. Based on a literature study concerning the ideal information security and control situation and the results of the three sets of questionnaires it was possible to determine the gap, problem areas and issues of information security and control at the manufacturing company. The research clearly indicated that numerous areas for improvement exist and therefore proposes a framework for the management of information security. Although a completely secure information system may not be attainable, the valuable information asset can to a large extent be protected through proper management.

Introduction

The 2000s are characterised by continual and rapid change in technology. One specific aspect that is having a major impact on everyday life is the phenomenon generally known as the information explosion. Information has in fact become the essential ingredient for profits and success (Du Toit, 1992:9). In the bid to use this massive volume of information economically and effectively, computers increasingly play a more significant role. This increased dependence on computer technology and computer-based information systems in organisations to enable diverse business activities, has redefined corporate risk and thus necessitated closer scrutiny of security practices and procedures to offset the risk inherent in giving more people access to computer systems (Lubbe & Armstrong, 1995:19; Pottas, 1995: vi, 3; Von Solms, 1993:1).

Requirements for security have escalated to the protection of a myriad of autonomous and integrated information systems, data and information residing on mainframes, minicomputers, servers, workstations and personal computers (Scott, 1996:1; Eloff, 1980:1). It is therefore necessary that the confidentiality, integrity and availability of information should be ensured on all levels (Menzies, 1993: 164-165).

Despite numerous management claims that information is one of the most valuable and strategic corporate assets (Pfleeger, 1989:299; also compare Clarke, 1976:1; Davis & Olson, 1987:216; Du Toit, 1992:7; Christoffersson, Ekhall, Fåk, Herda, Matgtila, Price, & Widman, 1988:1), there is often not much pressure from executive level or adequate funding to ensure that information stored on computer systems is protected from bumbling, break-ins, electronic fraud, viruses, and natural disasters (compare Louw, 1990:213; Pfleeger, 1989:2; Rilley, 1981:5; Thibodeau, 1997). Many organisations do not implement an active information security plan, and when implemented it is often done half-heartedly (Van Dyk, 1990:18). It is also true that management often conceal the truth about the status of information security in their organisations (Stang, 1992:16). Although management may be well aware of the shortcomings and dangers with regard to information security, they often rationalise and believe their own fabrication (Highland, 1993:2).

Linked to this apathy towards security by senior management, De Ru (1992:3) pointed out, is the growing concern regarding the ability of current tools, methods, procedures, solutions, and human resources to meet the information security challenges and issues confronting management in the years to come (compare also Pfleeger, 1989:xix; Witten, 1990:105). While the use of information technology is increasing, misuse and security risks associated with the deployment of information technology are increasing even faster and often results in huge financial losses (Applegate, Austin & McFarlan, 2003:424; Rilley, 1981:2-3; Wong & Watt, 1990:1-2). Industrial espionage, fraud, crime and subterfuge are escalating in frequency and in adverse impact on victim organisations (Wong & Watt, 1990:2). It is also a well-known fact that computer crimes are increasingly becoming more sophisticated (Holton, 1996).

Besides all the above-mentioned problems, normal operating conditions and natural disasters (fire, water, and power failures) pose their own risks. Taken together with inherent flaws of fourth and fifth generation programming languages with respect to data control and validation, the powerfulness of search engines, audit trail and error recovery, as well as the increased network sharing with outside organisations, office automation, electronic mail, electronic data interchange, and unattended operation, it is quite clear that top management can no longer ignore the security of the valuable information asset (compare Denning, 1990:iii-iv; Wong & Watt, 1990:15-20). Although the Communications and Electronic Transactions Act, Act 25 of 2002 (South Africa, 2002) brought some improvement, South African legislature is still relatively inadequate (compare Snyman, 1999:4). If it is born in mind that South African legislation is not moving fast enough to deter hackers or fraudsters (Middleton, 2001:1), it becomes evident that many hackers go undetected and unprosecuted (Camp, 2000:54; Campling, 1997:1).

Information security can thus not remain a technical issue, delegated to technical specialists, but will have to become a business issue, addressed by corporate executive management (Wong & Watt, 1990:20). This urgency for the addressing of information security by senior management is furthermore highlighted by the inherent danger of the continuing departure from traditional mainframe computing to departmental computing, distributed platforms, decentralised security, the 'openness' of today's systems architectures, greater accessibility, interconnectivity, networks, and a large scale connection to the relatively insecure Internet (Claassen, 1994:1-1; Cohan, 1999:88; Eloff, 1995:39; Heydenrych, 1996:16; Menaugh, 1997; Smith, 1996; Sundaram, 1998).

A South African case study

Because of the above-mentioned aspects, it is of the utmost importance that information security is addressed in every organisation. The urgent necessity for information security is also found in the highly competitive manufacturing world. This article will therefore report on a study of information security and control at a large and diversified manufacturing company that produces a rich variety of products.

The company makes extensive use of computerised information, local and wide area networks, the Internet, as well as distributed computing and dial-in lines, which emphasise the importance and necessity to study the current level of information security and control. This connectivity dramatically increases the vulnerability of the information resource. Therefore some information security control measures, for example identification procedures and passwords, were implemented. A proxy server, firewall, as well as authentication and identification procedures, and passwords protect access to the Internet.

Certain dynamic changes in the computer environment of the company lead to an increase in information security risks and threats. Some of the more important changes were

- a dramatic increase in the use of personal computers;
- an increase in the use of local and wide area networks;
- an ever-increasing dependency on information;
- totally new information needs;
- an increasing complexity and integration of systems and technology; and
- an increasing end user involvement.

These changes in the information technology environment inevitably lead to an increase in the following information security risks and threats: fraud and theft; violation of information privacy and security; loss of resources and finances; sabotage and industrial espionage; and misuse of assets and resources.

Evaluating information security

There is little doubt that security problems will increase because of the dramatic growth in information technology. Computer crime and fraud will become more sophisticated and popular, as organisations become more and more dependent on information systems. If senior management therefore does not address the various information security threats, it can lead to a variety of information security problems and computer crimes.

The major information security threats currently experienced are external threats, internal threats, accidental threats, hardware misuse, computer fraud and crime, intrusions, masquerading, pest programs, bypasses, active misuse, passive misuse, and indirect misuse (Applegate *et al*., 2003:433-439). Although it is not possible to build a completely secure information system and to eliminate all threats and problems, it is possible to minimise the impact and business disruption by following a total systems approach and by paying attention to risk analysis, risk monitoring and risk control.

Various information security controls can thus be implemented, for example administrative, physical, procedural, operational, information systems, systems development and last resort control measures. Synergy between the various components of information security is however a necessity.

To determine the state of information security at an organisation it is necessary to evaluate the various aspects that are threatened, as well as the level of implementation of the above mentioned control measures.

Methodology

The empirical research focused on the awareness of the ever-increasing information security risks, the effectiveness of the currently implemented security solutions, tools, available human resources, as well as the security concerns and problems at the manufacturing company.

For the purpose of the research, elements of survey-based feedback were used as a diagnostic approach. The main tool for the collection of data was three sets of questionnaires. Three groups were targeted for the distribution of the questionnaires, namely general computer users, departmental and functional heads, and information technology support personnel. The population was stratified (compare Huysamen, 1994:40-41; Lind & Mason, 1994:211-212) in order to determine three important perspectives, namely that of the general employees, management, and the information technology personnel. The stratification also ensured that general computer users did not have to answer management or specialised information technology questions. In all three groups the units of analysis (compare Huysamen, 1994:38) were the computer users at the manufacturing company.

Because the population of computer users is a finite population, it was decided to use the whole population for all three groups of computer users and not to make use of sampling techniques. If it is kept in mind that the average response to questionnaires is about thirty percent or lower, a sample would be too small to make valid deductions (compare Huysamen, 1994:149-150). A total of 121 computer users were thus identified as the population. The questionnaires were furnished to all computer users at the manufacturing company according to a list of the relevant units of analysis.

The first part of the questionnaires mainly obtained biographical data of respondents and thus included questions concerning the demographic and personal particulars of users, while the rest of the questionnaires measured the general perception of the main aspects of information security at the manufacturing company.

After the questionnaires were received back all responses were carefully scrutinised for completeness, consistency and errors (compare Berenson & Levine, 1996:31), and to eliminate questionable data (compare Steyn, Smit, Du Toit, & Strasheim, 1994:3). Out of the total of 121 questionnaires distributed, 56 questionnaires were received back, which means a 46.3% total response rate. The response rates for the three respective groups are presented in Table 1.

The differences in the composition of the population and the composition of the respondents were negligible as can be seen from Table 2 on the next page.

The responses included nominal data (responses to the demographic questions), as well as ordinal data on a four-point Likert scale. The processing of the data was done by means of the Statistica for Windows program. In the processing of the data the major emphasis was on descriptive statistics to organise and summarise the numerical data (compare Lind & Mason 1994: 5-6).

Contingency analysis was used to establish whether the demographic variables had an effect on the nominal data collected. A frequency distribution analysis and analysis of variance was used to identify the major information security problems that users experience, and to investigate the variation in the interval scaled variables. In order to evaluate the respective statements and questions, the following statistical procedures were performed: frequency distributions; histograms; the arithmetic mean, which is the most commonly used average or measure of central tendency (Berenson & Levine, 1996:106); and the 95% confidence intervals, which states the range within which the total population parameter is expected to lie (Berenson & Levine, 1996:344-348; Lind & Mason, 1994:225-228). To determine the representativeness and reliability of the mean, the standard deviation as measure of dispersion was calculated for each question (Berenson & Levine, 1996:120-124). However, when a few extremely large and extremely small items are encountered in a set of data, the mean might not be an appropriate measure of central tendency (Lind & Mason, 1994:62). To overcome this problem and to determine the shape or symmetry of the frequency distribution, the degree of skewness of the distribution was determined.

Results

Fourteen aspects of information security were evaluated to determine the overall state of information security at the manufacturing company. The results of the evaluation described above are concisely summarised in Table 3.

From Table 3 it is evident that in all fourteen areas the manufacturing company experienced problems with regard to information security. However, based on the number of problems experienced and the overall evaluation, some of the areas need more attention than others. A more detailed discussion of the security problems that were uncovered follows below.

Microcomputer security

Microcomputer security is one aspect that seriously needs attention. No regular audit and review or a microcomputer security policy existed. Neither were backups, control of data, control of proprietary software, or encryption on an adequate level. When backups on microcomputers were made, version numbers and creation dates were not recorded.

Administrative security

Information security awareness – security standards were not communicated enough. Regular updates and reminders on information security are necessary to keep employees informed. Training of new employees in information security was almost non-existent and should be addressed.

Information security policy – no formal information security document existed. Documentation on security matters did not really exist and were mostly left to the initiative and competence of employees. Formulated information security objectives or action plans also could not be traced. Plans were not co-ordinated.

Table 1: Response rate

Group	Total number of computer users	Number of respondents	Percentage
General computer users	81	34	41,98%
Functional and departmental heads	35	18	51,43%
Information technology support personnel	5	4	80,00%
Total	**121**	**56**	**46,28%**

Table 2: Differences between the composition of the population and respondents

Group	Population	Respondents	Difference
General computer users	66,94%	60,71%	-6,23%
Departmental and functional heads	28,93%	32,14%	3,21%
Information technology support personnel	4,13%	7,14%	3,01%

Table 3: Evaluation of information security according to fourteen key areas

Criterion	Aspects evaluated	Significant problems
Microcomputer security	8	6
Administrative security	25	16
Procedural security	15	8
Management of information security	12	6
Operational security	33	16
Contingency planning and disaster recovery	43	14
Computer centre security	10	3
Network security	28	8
General security	50	13
Internet security	8	2
Virus security	12	3
Information system security	29	6
Physical security	69	13
Systems development security	24	4

Personnel controls – the dividing of responsibilities was implemented as a control measure. Attention should, however, be paid to background checks on all new employees, rotation of critical jobs, non-disclosure agreements, and the enforcement of a clean desk policy.

Security conscious environment – the general perception is that stringent security measures operate. This perception does not, however, hold true for information security. The overall environment was all but information security conscious as was evident from the inadequate supervision of visitors, courier security, use of photocopiers and the mailroom.

Procedural security

Logical access security – although authorisation controls were effective, many computers were left on when unattended and employees did not log off from the network when leaving the personal computer for more than fifteen minutes. This minimised the value of access control. Although passwords were unique it should be changed more regularly. Multiple log-ons should not be allowed. External or remote access (dial-in) was not according to accepted security standards.

Data security – there was no specific person who reviewed new or existing data in terms of classifying it for storage and filing purposes or for the dissemination to potential users. Most of the data and information was available to all persons. There were a number of informal procedures, which did operate to limit personnel's access to certain confidential information. The classification of data, consistency across environments, standards, database encryption, off-site backup, the protection and disposal of sensitive documents, and the review of exceptions, need attention.

Management of information security

Attention will have to be paid to winning top management commitment. Although it seems that information management is important to senior management and that they accept their responsibility, it became evident that top management does not view the vulnerability of this strategic asset as a critical performance area. The result is that neither enough attention is paid to this problem, nor is enough funds allocated to do the job. Quite a few management aspects therefore need to be addressed.

Provision of funds for information security – a major obstacle to information security being addressed is the lack of budget. The budget is the formalisation of the monetary implications of the business plans. The budget at the manufacturing company therefore reflected the relative lack of concern for information security at top management level.

Despite the high physical asset value of the computer systems, the budget had no specific item referring to information security.

Security planning – another major obstacle to information security is the fact that security planning did not form part of the total strategic and business planning. In fact there was a lack of a total information security plan on the strategic level. Information security strategies also need to be more effective and aligned with business strategies. The effectiveness of the security administration needs attention.

Assignment of specific responsibility – the information technology manager is responsible for information security, but because of an overload of work cannot pay justice to this very important task. Top management has not yet deemed it necessary to have a specialist information security manager to meet its needs in the information field. Although the information technology manager has created a personnel structure under him, no specific person has been assigned the task of information security.

Assessment of organisational vulnerabilities, threats and risks – neither the management nor the information technology manager had any formal assessment of vulnerabilities, threats and associated risks to which the information resource is exposed. Until now little thought has been given to vulnerabilities such as fraud, theft, sabotage, espionage and other information security problems.

Investigation of information security countermeasures – no active investigation of available and new countermeasures took place. A formal record of information security countermeasures could not be found.

Risk management strategy – as a result of not having a formal assessment of vulnerabilities, threats and countermeasures, a formal risk management strategy to reduce the information security problem, did not exist. Risk management was often done on an ad hoc basis or as a result of some incident.

Implementation of countermeasures – because of the lack of a well defined risk management strategy and plan, there were no specific plans laid down to implement information security countermeasures. Countermeasures were often implemented when a person or incident requires some defensive attention to be given to a specific problem area.

Monitoring and reviewing information security effectiveness – the security management function did no specific monitoring of its own accord in the area of information security. No regular audits of information security existed. A disaster recovery plan existed, but was never tested.

Operational security

Although most computer users viewed operations and maintenance security as of a high standard, quite a few aspects need to be corrected.

Maintenance security – although mostly in order, procedures were not documented adequately; neither was enough being done about the training of personnel regarding emergencies. The separation of maintenance responsibilities was inadequate. Unauthorised parting and changing of sensitive programs were not always prevented. The request for updates was not reviewed by an independent party.

Tape and disk library security – the management of the tape and disk library was not up to standards. The alarm and sprinkler system should be thoroughly revised. Degaussing of old tapes and disks should be implemented. Tapes authorised for release but not found, and tapes for which the responsible person was not identified, should be identified and resolved. Version numbers and creation dates for backups were not recorded. Programs and documentation were not always stored in a secure location. The inventory list should be updated more frequently and sign-out logs should be strictly used. The old master was not always retained and monitored by the librarian.

Support service security – the security of support services is an aspect of information security that was assessed very low. Non-disclosure agreements were not used. Maintenance visitors were not supervised.

Contingency planning and disaster recovery

Contingency plan and backup – an aspect that was rated very negatively is contingency planning. Although some aspects of the contingency plan were in order, vital records have not been identified and classified, which made the orderly removal of important records in the event of a disaster impossible. The present contingency plan was not at all effective, did not contain clear instructions, and did not address the various levels of service interruption. Another alarming aspect is that the disaster recovery plan was not regularly tested, neither were there procedures to regularly update the plan. Overall user involvement, without which the successful implementation of a disaster recovery plan is almost impossible, was lacking. Alternative facilities or a disaster recovery site did not exist, with the result that resilience was very low and continuation of work in case of a disaster would be very unlikely.

Natural disaster security – several precautions have been taken. Aspects that still need to be addressed are the fact that the walls, doors, partitions and floors of the server room will probably not withstand the spread of a fire, and that the sprinkling system cannot be pre-empted while personnel extinguish the fire manually to prevent machine damage.

High quality self-locking doors with ‘panic bars’ on the inside at the server room were lacking. Access control to the building by the guards and electronic access control to the building need improvement because of the possibility of mob attacks.

Disaster recovery – The company did not have an effective planned incident response or response team when an intruder is detected in the computer network. Consideration

should be given to the establishing of a detailed incident response plan and a small response team.

Insurance against power failures, errors, data and business losses were inadequate.

Computer centre security

The operations log that records any significant events and actions was not constantly maintained or inspected daily by management. A dangerous practise was that visitors to the computer area were not escorted. The level of physical access security, after hour access control and control of the removal of materials from the server area were inadequate and need attention. Access control, however, begins with access control to the building by the security guards and electronic access control, which both need improvement.

Network security

Although network security was perceived to be effective, the network was not adequately protected from attacks or constantly monitored. Serious shortcomings were that critical transmitted information was not encrypted, logins of a given user were not restricted to a specified workstation, the change of passwords was not restricted to the user only, and start-up scripts were not imposed. Another aspect that should be addressed is sound documentation, which was lacking.

General security

General security of the computer systems is quite good, except that of desktop or microcomputers, remote computing and laptops, which certainly should receive attention.

General information security measures, which are regularly used, are virus detection software, secure modems, firewalls, and network access control software. Attention will have to be paid to token-based passwords, personal computer access controls, personal computer hardware security devices, terminal key locks, lock words, redundant communication, business continuity planning software, and security evaluation software.

It also became apparent that single sign-on software, signature verification, telecommunications encryption, biometric authentication, message authentication, file encryption, and public-key cryptography are never used and should be investigated as a means of protection. Although non-disclosure agreements by personnel are not regarded as important, it deserves attention.

Internet security

Internet security seems to be adequate. Passwords and firewalls are used as control techniques. Encryption is not used and should be considered in the case of critical information.

Virus security

Computer viruses remain an imminent threat and were widely experienced by employees and mostly affected microcomputers and to a lesser extent also the servers. Although several control measures are being used, a documented virus security policy, a definition of potential losses, and documented safe user practices did not exist. The major consequences of the computer virus attacks were a loss of time, functionality and data. Virus protection, especially on microcomputers, will have to be improved dramatically.

Information system security

Security of sensitive programs – although negatively evaluated, nothing could be concluded with certainty regarding the security of sensitive programs like the payroll, accounts payable, fixed assets, purchasing, and inventory control. These aspects probably need some attention.

Input/output security – effective controls for point of origin review of the rejected sensitive transactions, and the correcting of errors in input/output at the point of origin have been established, but will need regular auditing.

Storage security – there is no formal review of existing systems on a regular basis to determine whether redundant information is being kept. Version numbers and creation dates are not recorded. No classification scheme exists. Consistency across environments and data encryption are lacking. No off-site backups of data are kept.

Telecommunications security – telecommunications security is adequate, except that encryption is not always used in the case of critical information.

Physical security

Although the general perception is that physical security is of a high standard, this is however not exactly true as is evident from the following shortcomings.

Protection against natural disasters – The present walls, doors, partitions, and floors of the server areas will not resist the spread of fire. Sprinkling can unfortunately not be pre-empted to allow personnel to take corrective action and to limit water damage. The number of sprinklers is inadequate.

Physical access control – No high quality self-locking doors are being used and electronic access control is not effective. Especially access control in server areas and after hours access control need attention. Access control to the building by the security guards is also ineffective. All these problems mainly boil down to the fact that physical access control is not effectively managed. Inadequate controls over the removal of materials lead to losses.

Remote site security – The level of security of remote sites is inadequate and need attention.

Systems development security

Information systems development and documentation security is basically on an acceptable standard, but a few aspects will have to be addressed by management.

Security of new programs and program changes - although all revisions are supported by written requests that need to be approved by management, procedures that prevent programs from being changed without consent of the user's department do not exist and should be implemented. Unfortunately no full history of changes is maintained.

Documentation documentation security is poor. Documentation standards are not strictly enforced before new systems are implemented or existing ones are changed. Program documentation is also not adequately maintained. Classification schemes, disposal of sensitive documentation, protection of sensitive documentation and general standards need to be addressed.

A managerial information security framework

From the above discussion it is evident that a lack of security was found at the manufacturing company in all three basic aspects of security, namely confidentiality, integrity and availability (see Alexander, 1995:30; Louw, 1990:76-77; Menzies, 1993:164-165; Olivier, 1991:9; Pritchard, 1979:13 for the three basic aspects of information security). To remain competitive in the highly competitive market the company will have to implement an information security framework and plan. Eventually this plan will have to be translated into detailed action plans with appointed responsible persons at all strategic business units.

A possible framework for the management of information security is displayed in Figure 1 on the next page.

From Figure 1 it is evident that this managerial framework for information security consists of the following major aspects.

Senior management involvement

Information security is a deliberate decision, rather than relying on security through obscurity. Senior management should recognise information resources as essential organisational assets that must be protected, educate themselves on security related issues, and take responsibility for decisions in this area. The efforts of high-level executives to understand and manage risks help to ensure that information security is taken seriously at lower levels in the organisation and that security programs have adequate resources.

The responsibility for information security thus rests with senior management to install into their organisation a defensive threshold, which is high enough to make the investment in time and effort unprofitable to any potential adversary. Top management effects their involvement by defining and communicating a security policy, by allocating specific responsibilities to appointed people, by making resources available for the continual upkeep of information security and control, and by constantly monitoring and reviewing information security effectiveness.

Information security policy

Senior management implements a security framework and plan by starting off with the formulation of a corporate security policy and strategy that forms part of, and is aligned to, the total business strategy.

The following steps can be followed in developing an information security policy (Stefanec, 2002:13-18):

- Perform a threat and risk analysis for the organisation to determine the level of security that must be implemented. Practical risk assessment procedures are developed that link information security to business needs. The assessment should include environmental threats; hardware, software and liveware problems and failures; fraud and theft; as well as sabotage and industrial espionage.

- Define a security policy for the entire organisation and use it as a guide for information security architecture. The architecture rest on the following points: confidentiality, integrity, availability, assurance and enforcement and is determined by an audit of the corporate information security infrastructure. The audit includes an analysis of the confidentiality and criticality of computer resources, an assessment of all the various information security threats, risks and vulnerabilities, as well as an investigation of the available countermeasures, safeguards and controls.

- Create an information security implementation plan. Once the audit is completed, an information security plan and budget is submitted for approval by management. The budget for information security should be in line with the asset value of the information and information technology of the organisation and should enable the organisation to plan and set goals for information security programs. The budget should cover central staff salaries, training, and security software and hardware. In the establishment of a defensive threshold to deter potential adversaries, cost and benefits will have to be traded off against one another.

- Assign accountability. Programme and business managers should be made accountable for information security. Business managers should be held accountable for managing the information security risks associated with their operations, just as they are held accountable for other business risks. Security specialists in these organisations should have an advisory role, and it includes keeping the management informed about risks. Similarly, program managers must determine which of their information resources are the most sensitive and assess the impact of security problems.

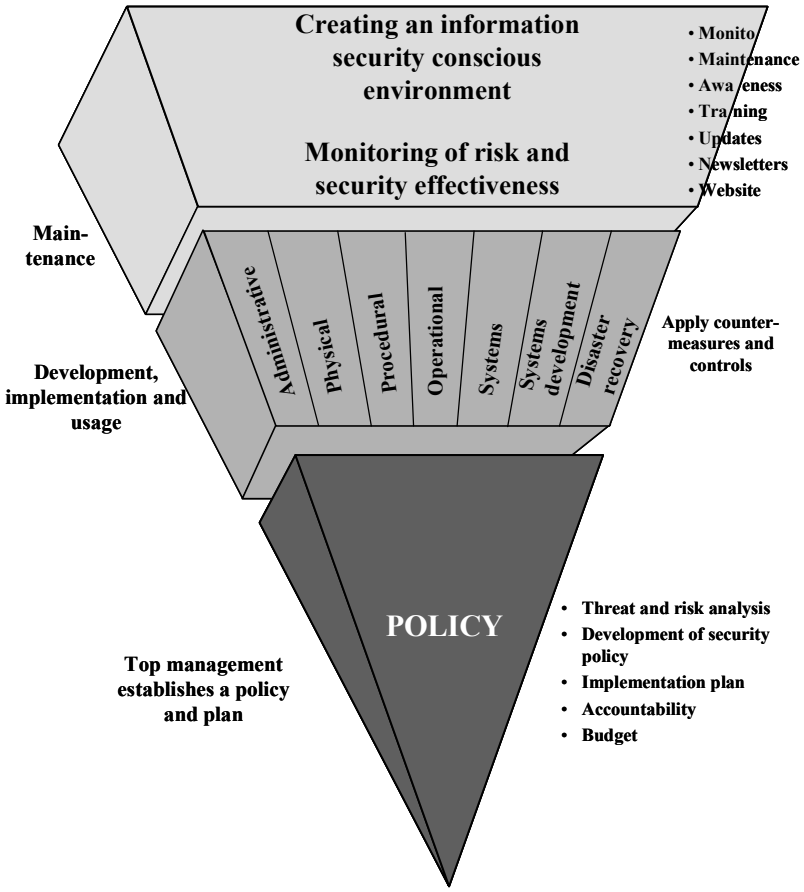

Figure 1: Framework for the management of information security

Aspects that need to be considered in the information security policy are: security aspects that includes aspects of strategic nature, as well as the long term impact and implications; insurance aspects that involves the management of asset and resource risk in order to ensure the survival and effective functioning of the organisation; aspects regarding the organisation structure, which comprises personnel practise, as well as the structure within which the computer environment is organised; contingency and disaster recovery aspects; systems development aspects that describes the methodology to successfully develop application systems; and maintenance aspects.

The formulation of policy is unfortunately not a once-off exercise and should be reviewed constantly in order to ensure that it is still appropriate to the ever-changing security environment.

Countermeasures

After the establishment of policies and strategies, it is necessary for successful implementation of the required administrative, physical, procedural, operational, information systems, systems development controls, as well as controls of last resort. A possibility is to follow an architectural approach. An architectural approach implies a proactive understanding of how information is used throughout the organisation and its corresponding security requirements. Thus the following two aspects must be secured:

- Continuity of computing services (the availability aspect of security) by the establishment of strict maintenance service standards, the provision of redundant support services, strict change control standards, strict back up procedures, and training of employees.

- Control of access to information (the confidentiality and integrity aspects) through logical access control and user accountability. Authentication can be obtained through passwords or third party authentication software.

Constant monitoring

Due to the fact that information security is a constant process, continuous attention should be paid to security. To determine the effectiveness of the control measures and to enforce the implemented safeguards the security manager and his personnel do continuous monitoring of risk and security effectiveness, regular security audits, and if necessary maintenance work to ensure the required level of information security and compliance with the information security policy.

Resource elements which can be used by management for the application and monitoring of information security may include:

- A security committee and team to co-ordinate and implement all aspects regarding information security.
- Internal and external audits to ensure that information security meets the policy, procedures, and rules stipulated by management.
- Quality assurance to ensure that standards and prerequisites will be met.
- Security administration that administrates and regulates information security.

Creating an information security conscious environment

Unlike popular believe, the successful protection of information does not hinge entirely on technological developments, but is also a matter of security awareness by senior management and all employees. It is therefore important that management initiates a security awareness program by training management and all new employees in information security, by providing regular information security updates and newsletters, and by creating an information security inducive environment. Many of the security problems and threats can be eliminated if the ordinary employee takes it on him- or herself to be part of the solution to information security.

An inducive environment to facilitate information security can be created by doing the following:

- Starting with a comprehensive awareness program. Attention-getting and user-friendly techniques should be used in the awareness programme. Techniques can include intranet web sites that explain policies, standards, procedures; alerts and special notices; awareness videos with messages from top managers about the security program; interactive presentations by security staff with various user groups; security awareness days; and products with security related slogans.
- Training and education programs, which emphasise the information security threats and vulnerabilities, faced by the organisation. All new employees should go through an introductory computer security course, with a refresher course at least every year;
- Thorough planning of all aspects of information security;.
- Clear information security policy statements, standards and guidelines.
- Well documented procedures for information security.
- Implementation of information security.
- Top management commitment to the strict enforcing of discipline with regard to information security.

Conclusion

The present age is an age of information insecurity. Therefore organisations will have to accept that security is a cost of doing business. Since information security is a moving target where perpetrators are constantly looking for new ways to attack, information security is not something a company can do once and then forget about. But ensuring information security on an enterprise wide network is often practically an elusive goal and may even be unattainable because in today's distributed networked environment open access to information takes precedence over the protection of information integrity and confidentiality. However, various measures and controls can be implemented to improve information security.

There is little doubt that information security is more of a management issue than a technical issue and that it should be managed according to the level of risk and potential threats to the organisation. The type and profile of the organisation as well as its business and its objectives influence the level of risk. The higher the competitive environment of the organisation, the more information it needs and thus the security risks increase. A fairly low profile organisation with a low level of competitive environment has a low security need. If this statement is used as a platform, it can then be said that that information security can be managed through a series of general and application controls that can prevent threats, or detect and control the effects of damage if a disaster, security violation or failure takes place. To ensure efficiency of these controls regular audits, monitoring and critical incidence reproduction tests should be carried out (Bryson, 1997:341).

Perhaps security is a journey without end. Menaugh (1997) said that having the right mind-set for information security is not 'a question of whether or not you're paranoid, it is rather whether you're paranoid enough'. In this new age of cybercrime, probably the only totally secure computer system is the one that has been switched off. However, if information security is implemented properly so that it does not overkill, ignore or produce a false sense of security, it will limit the risks to which the organisation is exposed.

Therefore, if the researched manufacturing company is any indication of the state of information security in manufacturing organisations, information security in the manufacturing environment in South Africa should receive much more attention and investment. Unlike the USA who took information security much more serious after the September 11, 2001 terrorist attacks (Applegate *et al.,* 2003:432), South Africa need a more structured approach to information security. Management will have to take the escalating threat to information security much more serious by building defences to secure companies' information related assets. It should never be a once-off issue, but should form part of the corporate business strategy. Information security is not an event, but a constant and complex process.

However, to determine the state of information security in South Africa a much more comprehensive study involving many more companies will have to be undertaken.

References

Alexander, M. 1995. 'The real security threat: The enemy within', *Datamation*, **41**(13): 30-33.

Applegate, L.M., Austin, R.D. & McFarlan, F.W. 2003. *Corporate information strategy and management.* 6th Edition. Boston: McGraw-Hill/Irwin.

Berenson, M.L. & Levine, D.M. 1996. *Basic business statistics: Concepts and applications.* 6th Edition. Englewood Cliffs: Prentice-Hall International.

Bryson, J. 1997. *Managing information services: An integrated approach.* Aldershot: Gower Publishing.

Camp, L.J. 2000. *Trust and risk in Internet commerce.* London: MIT Press.

Campling, R. 1997. 'Computer crime is a profitable business', *Computer week*, **20**(38): 1.

Christofferson, P., Ekhall, S., Fåk, V., Herda, S., Matgtila, P., Price, W. & Widman, K. 1988. *Crypto users' handbook: A guide for implementers of cryptographic protection in computer systems.* Amsterdam: Elsevier Science Publishers.

Claassen, G.J. 1994. **'**Security model, protocols and architecture for open distributed systems'. Pretoria: University of Pretoria. (Ph.D Thesis.)

Clarke, L.G. 1976. **'**Die beplanning en beheer van 'n bestuursinligtingstelsel wat geskep word met die klem op strategiese beplanning en die uitwerking wat dit het op die huishouding van die onderneming'. Pretoria: Universiteit van Pretoria. (M.B.A Skripsie.)

Clement, J.H. 1992. **'**Evaluation and control of information technology investments'. Johannesburg: University of the Witwatersrand. (M.B.A. Dissertation.)

Cohan, P.S. 1999. *Net Profit: How to invest and compete in the real world of Internet business.* San Francisco: Jossey-Bass Inc. Publishers.

Davis, B.D. & Olson, M.H. 1987. *Management information systems: Conceptual foundations, structure and development.* 3rd Edition. New York: McGraw-Hill.

Denning, P.J. (Ed.). 1990. *Computers under attack: Intruders, worms, and viruses.* New York: ACM Press.

De Ru, W.G. 1992. **'**Die toepassing van ekspertstelseltegnologie binne inligtingsekerheid'. Johannesburg: Randse Afrikaanse Universiteit. (M.Sc. Verhandeling.)

Du Toit, L.M. 1992. **'**'n Model vir inligtingsekerheidsdokumentasie'. Johannesburg: Randse Afrikaanse Universiteit. (M.Sc. Verhandeling.)

Eloff, J.H.P. 1980. **'**Rekenaarsekuriteit met besondere verwysing na die programmatuuraspek'. Johannesburg: Randse Afrikaanse Universiteit. (M.Sc. Verhandeling.)

Eloff, J. 1995. 'Information security: State-of-the-art overview', *Information Technology Review*, **2**(11): 39-40.

Fisher, J. 1998a. 'Java and JavaScript vulnerabilities', CIAC notes 96-01, March 18 1996. [online]: URL:http://www.ciac.org/ciac/notes/notes96-01.shtml.

Fisher, J. 1998b. 'Security and web search engines', CIAC notes 96-01, March 18 1996. [online]: URL:http://www.ciac.org/ciac/notes/notes96-01.shtml.

Heydenrych, F. 1996. 'When will the Internet grow up?', *Information Technology Review*, **3**(2): 12-13, 15-16, 19.

Highland, H.J. 1993. 'A view of information security tomorrow'. **In** Dougall, E.G., (Ed.). *Computer security: Proceedings of the IFIP TC11 ninth international conference on information security, IFIP/Sec'93, Toronto, Canada, 12-14 May, 1993*. Amsterdam: North-Holland.

Holton, G. 1996. 'Computer viruses are out there but you may still surf the Internet with confidence'. **In** *Networld & Landaba 96*. [CD-ROM.]

Huysamen, G.K. 1994. *Methodology for the social and behavioural sciences.* Halfway House: Southern.

Lind, D.A. & Mason, R.D. 1994. *Business statistics for business and economics.* Burr Ridge: Irwin.

Louw, E. 1990. **'**Computer viruses: A management concern'. Johannesburg: University of the Witwatersrand. (M.B.A. Dissertation.)

Lubbe, S. & Armstrong, G. 1995. **'**Computer crime and the measures of detection and prevention of such crime', *Vital*, **10**(1): 19-31.

Menaugh, M. 1997. 'First line of defence'. [online] URL: http://www.computerworld.com/search/AT-html/9702/970210Slcar0210a html.

Menzies, R. 1993. 'Information systems security'. **In** Peppard, J. (Ed.). *IT strategy for business.* London: Pitman.

Middleton, G. 2001. 'SA hacking web site one of global favourites'. [online] URL:http://www.istrategy.co.za/itweb/january01/4f/index.shtml.

Olivier, M.S. 1991. 'Secure object-oriented databases'. Johannesburg: Rand Afrikaans University. (Ph.D Thesis.)

Pfleeger, C.P. 1989. *Security in computing.* Englewood Cliffs: Prentice Hall.

Pottas, D. 1995. **'**The automatic generation of information security profiles'. Johannesburg: Rand Afrikaans University. (Ph.D Theis.)

Pritchard, J.A.T. 1979. *Security in on-line systems*. Manchester: NCC Publications.

Rilley, C.D. 1981. **'**A managerial framework for the evaluation of information security and privacy in a large chemical organisation'. Pretoria: UNISA. (M.B.L. Dissertation.)

Scott, R.F. 1996. 'Secure data transmission between computers*'*. Durban: University of Natal. (M.Sc. Eng. Dissertation.)

Smith, J. 1996. **'**The security impact of remote and Internet access on corporate networks'. **In** *Networld & Landaba 96*. [CD-ROM.]

Snyman, C.M. 1999. 'Fighting computer crime within organisations: A managerial and legal perspective*'*. Potchefstroom University. (MBA Dissertation.)

Stefanec, G.L. 2002. *Information security best practises: 205 basic rules.* Boston: Butterworth-Heinemann.

South Africa. 2002. *Electronic communications and transactions act: Act 25 of 2002.* Pretoria: Government Press.

Stang, D.J. 1992. *Dealing with network security threats: Securing your LAN.* Washington: International Computer Security Association.

Steyn, A.G.W., Smit, C.F., Du Toit, S.H.C. & Strasheim, C. 1994. *Moderne statistiek vir die praktyk.* Pretoria: J.L. van Schaik.

Sundaram, A. 1998. *An introduction to intrusion detection.* Paper published by ACM crossroads and technology manager. [online] URL:http://www.cs.purdue.edu/homes/sundaram/papers/intrus.html.

Thibodeau, P. 1997. **'**Technology forum international conference held to address Internet security, New York, January 1997*'*. [online] URL:http://www.computerworld.com /search/AT-html/9701/970122conferencesecurity.html.

Van Dyk, P. 1990. **'**Rekenaarsekerheid in mikrorekenaarstelsels.' Johannesburg: Randse Afrikaanse Universiteit. (M.Sc. Verhandeling.)

Von Solms, R. 1993. **'**Information security management: Processes and metrics*'*. Johannesburg: Rand Afrikaans University. (D.Sc. Thesis.)

Witten, I.H. 1990. **'**Computer (in)security: Infiltrating open systems'. **In** Denning, P.J. (Ed.). *Computers under attack: Intruders, worms, and viruses.* New York: ACM Press.

Wong, K. & Watt, S. 1990. *Managing information security: A non-technical management guide.* Oxford: Elsevier Science Publishers.