THE ROLE OF REAL-TIME INFORMATION IN RISK MANAGEMENT

Hilton Cameron[1] and Reinhardt Botha[2]

[1,2]Department of Business Information Systems, Port Elizabeth Technikon, South Africa

[1]hilton@hella.co.za, +27 41 9953034, Private Bag X6011, Port Elizabeth, 6000

[2]rbotha@computer.org, +27 41 5043669, Private Bag X6011, Port Elizabeth, 6000

ABSTRACT

Information Security is a growing concern in today's business environment. It is not easy for organisations to determine the security threats with which they are faced accurately. In addition to this, organisations also face the difficult task of determining the optimal amount to invest in order to protect themselves adequately.

Risk management may be used to assist organisations in deciding how much to secure their information technology environment and whether the cost will be justified by the resultant benefit. Risk, in this case, is the possibility of an event occurring which would reduce the value of the business.

The most ideal situation is to make use of real-time monitoring to monitor an organisations security risks continually. In this way security personnel can be alerted timeously and corrective measures can be put in place. In addition to operational issues, real-time measuring can also pickup trends, which can assist with tactical and strategic planning.

KEYWORDS

Information Security, Risk Management, Corporate Governance, Real-Time

THE ROLE OF REAL-TIME INFORMATION IN RISK MANAGEMENT

1 INTRODUCTION

Everyone is aware of the need for information security in today's global information society. Information is arguably among an organisation's most valuable assets, so its protection from predators from both within and outside is of great importance. In recent years, Information Technology (IT) Systems have become more susceptible to the many security threats, mainly because computers have become more interconnected and, thus, more interdependent and accessible to a greater number of individuals [16].

More and more we see information security in the news headlines, conveying the outbreak of a rapidly spreading internet worm or computer virus. The defacing of internet sites is also becoming common place in our society, not to mention the escalation of electronic fraud. Information security is a growing concern in the field of IT. There is an entire community of predators continually trying to penetrate the perimeter of one's IT systems.

So what exactly is information security? Dieter Gollmann [7, p. 3] defines security as follows: "Computer security deals with the techniques employed to maintain security within a computer system". However, ad-hoc security measures, which may well be useful, will not lead to an organisation being adequately secured. Proper security is an ongoing complex process [1, p. 11].

Information security aims to protect information assets, namely their confidentiality, integrity and availability [7, p. 5]. *Confidentiality* entails the safeguarding of information from unauthorised disclosure. Information *integrity* ensures the prevention of unauthorised modification of the information. *Availability* ensures that the information is not withheld and is always available to users.

Current day attackers have become quite sophisticated and have many tools at their disposal to infiltrate information systems [12, p. 42]. The attackers are commonly disgruntled teens, angry customers, ex-employees or just someone that wants to see if they can execute a successful attack [12, p. xix]. This has made the job of information security a lot more challenging. One should also bear in mind that it is often not the most valuable information that is compromised but the information that has the weakest protection.

An effective risk management process is a significant component of a successful information security program. The primary goal of an organisation's risk management process should be to protect not only an organisation's information assets but also its ability to perform its mission [15].

The authors believe that risk management and information security initiatives within organisations are not always aligned as well as they could be. This paper, therefore, considers the potential role of real-time information in risk management it suggests the use of a digital dashboard for providing real-time risk information.

2 RISK MANAGEMENT

In terms of business, risk is the possibility of an event occurring which would reduce the value of the business [3]. This event is known as an adverse event. These adverse events or risks usually have a cost associated with them, and this cost should be quantifiable for organisations. Information security breaches are clearly a form of adverse events and resultantly may cause losses for organisations. Information security is, therefore, a risk management discipline [3].

Every organisation, regardless of size, should be able to quantify the costs that are involved when its security is breached [5]. This can be achieved through risk management which essentially revolves around deciding how much to secure your IT environment and whether the expenditure will be justified by the benefit [9].

2.1 Why Utilise Risk Management

In today's competitive environment organisations cannot be uncertain about their vulnerabilities or be in doubt as to whether they have sufficient security measures in place. Risk management seeks to move beyond fear, uncertainty and doubt to a situation where organisations can quantify the likelihood of danger, estimate the damage that could occur and weigh the costs of safeguarding against these dangers [6]. Geer, Hoo, and Jaquith [6] point out that there are four realisations that are pushing organisations towards risk management.

Information Asset Fragility. Most organisations these days realise that their success depends largely on information. All the known occurrences of security breaches, corruption or destruction intensify their concern over this information dependency. The magnitude of information security and the need to safeguard against these threats is spreading.

Provable Security. Currently there are no consistent security metrics available. As a result of this organisations have difficulty in determining the suitability or effectiveness of different security options. Consequently, there is no quantifiable amount that an organisation should spend on security.

Cost Justification. The current economic climate and tightening of IT budgets means that there is less money available to spend on information security. Cost-benefit and return on investment calculations are becoming common place for investing in security measures.

Accountability. Various regulatory bodies are already mandating mechanisms for managing security risks. The Basel II Capital Accords, for example, will soon require banks to set aside capital reserves explicitly to cover operational risks, which include information security risks [2].

2.2 Risk Management in Practice

Risk management encompasses three main processes namely risk assessment, risk mitigation and ongoing risk evaluation [15]. Primarily organisations use risk management to determine the extent of the potential threat and the associated risk.

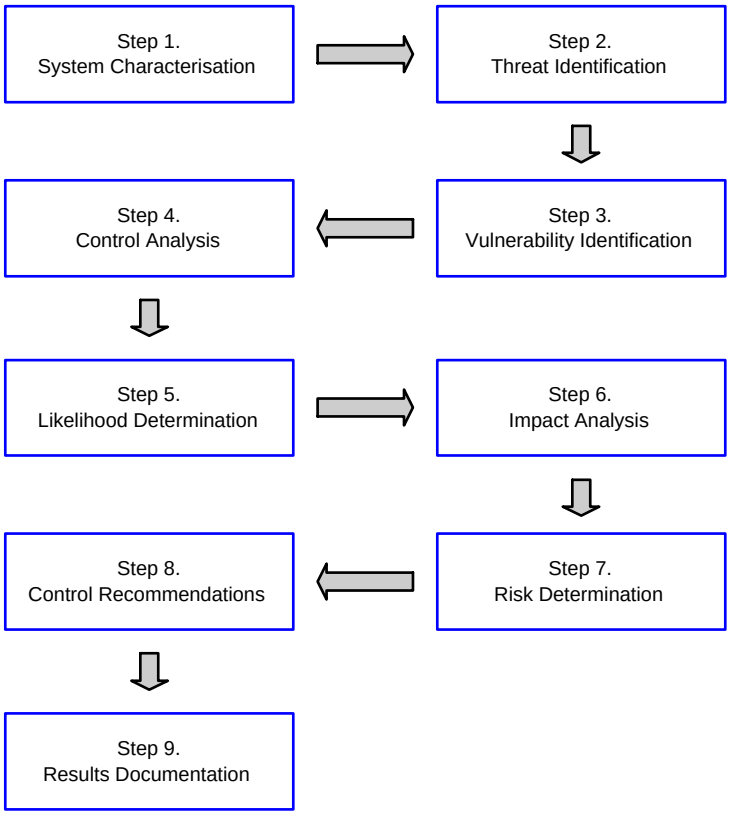

Figure 1: The Nine NIST Risk Assessment Phases

2.2.1 Risk Assessment

There are many different risk assessment techniques. The National Institute of Standards and Technology (NIST) proposes a risk assessment methodology which consists of nine unique phases. This methodology, which is depicted in figure 1, aims to assist with the better securing of IT systems [15]. Each phase is used to determine the extent of the potential threat and the associated risk. The output of the NIST assessment process helps to identify appropriate controls for reducing or eliminating risk during the following process, which is the risk mitigation process.

2.2.2 Risk Mitigation

Risk mitigation, the second process of the risk management guide proposed by NIST, involves prioritising, evaluating, and finally implementing the appropriate risk-reducing controls that are identified during the risk assessment process [15].

Because the elimination of all risk is usually unlikely or close to impossible, it is the responsibility of management to use the the most cost effective approach to implement the most appropriate controls that will decrease risk to an acceptable level, with the least impact on the organisation's resources.

2.2.3 Ongoing Risk Evaluation

The final process is ongoing risk evaluation. The risk management process is an ongoing and evolving process [15]. This is due to the fact that IT systems are continually changing. New hardware is installed, new and updated versions of software are used and the network itself is often expanded or updated. There are also often staff changes within a networked

organisation. This means that risks that were previously mitigated may once again be a concern, not to mention the fact that there are continually new risks surfacing in the world of IT.

Irrespective of the risk management approach used, the approach should provide for the provision of a risk action plan which will ensure for cost-effective controls and security measures that will mitigate the exposure to risks on an ongoing basis [9]. The risk action plan should distinguish the risk strategy with regards to risk avoidance, mitigation or acceptance [9].

The responsibility for risk management within an organisation lies with top management. In light of this, a brief discussion on corporate governance follows.

3 CORPORATE GOVERNANCE

Shareholders frequently delegate governance responsibilities to a board of directors. It is the corporate board's responsibility to ensure the continued success of the organisation. The board, therefore, is also responsible for the information security in the organisation [11]. The governance of IT falls within the realm of corporate governance as a whole, with IT governance becoming more prominent of late. IT governance is based on relationships and processes, which are used to guide and oversee an organisation. This is done so that the organisation may achieve its goals while at the same time cost effectively mitigating its risks.

IT governance is key to the success of organisational governance. The aim of IT governance should be to align IT with the organisational strategies and objectives [9]. In addition to this IT governance should also assist organisations to take full advantage of its information, and thereby gain a competitive advantage. The management of IT and its related risks is now being understood as an integral part of corporate governance. The IT Governance Institute [9], which authors COBIT, defines IT governance as follows: "A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprises goals by adding value while balancing risk versus return over IT and its processes."

The King Report on Corporate Governance for South Africa states that the board is responsible for the total risk management process [8]. It then goes on to state that management is accountable to the board and should design, implement and monitor the risk management process. Management, therefore, needs to identify what could go wrong and then put controls in place to prevent these risks. Once the controls are in place the controls should be continually monitored. In doing this management can gauge whether the controls are adequate. With efficient monitoring and alerting in place IT staff should be able to interrupt or at least contain a security breach that is in progress.

3.1 An Effective Monitoring Structure

An important part of IT governance is an effective monitoring or reporting structure. The structure should be hierarchical by nature with a clearly defined chain of command. A well thought out chain of command will assist in getting security incidents resolved faster and ensure that the correct people are notified [12, p. 370]. In addition to this staff members will only be notified of incidents that are pertinent to them, which prevents them from being flooded with unnecessary requests. Senior management are busy and

pressed for time. In light of this, there definitely needs to be some form of hierarchical reporting in place so as not to burden them with irrelevant information unnecessarily.

There are different levels of authority that will be involved in the monitoring structure. At the lowest level there will be the administrative type roles, such as the network administrators, server administrators and possibly a security administrator. There will then be a progression up the chain of command to security manager or IT manager. The chain will continue all the way to the top and will be structured according to the relevant organisation, with each level of the structure having its own responsibilities. Depending on the size of the organisation some of the levels or functions may be consolidated.

The idea behind the hierarchical monitoring structure is to have the most appropriate individual dealing with the incident first. Each group within the structure will be responsible for monitoring their own system. In the event where an incident is not dealt with, escalation up the chain of command is required.

A proper escalation procedure is often governed by time or severity [12, p. 372]. The more serious the incident the faster the response will need to be. Each different type of security incident will be assigned a particular route through the reporting structure. This incident should also have an appropriate time frame assigned to it. If the incident is not attended to within the predetermined time frame the incident should be escalated to the next level of authority.

Top management needs to be presented with highly summarised information which depicts trends. This type of information may assist them with strategic and tactical decision making. Administrative staff, on the other hand, need detailed transactional type information. They need the detailed information in order to deal with any day-to-day issues that may arise. Another common type of reporting that is required is the reports for middle management, the link between top management and the administrative staff. Middle management needs summarised information. They do, however, need the ability to drill down to operational level.

Top management, for instance, should not be concerned with the fact that a certain user has not chosen a secure password. The network administrator, however, should be notified and should take action to ensure that the user selects a more appropriate password. In the event that the network administrator does not deal with the insecure password issue there should be an escalation up the chain of command to ensure that it is dealt with. Although network administrators can put certain technical controls in place to control the passwords that users select. They can, for instance, define the minimum length of the password, or specify that the password must contain digits as well as numeric characters. These controls do not ensure that users will select a secure password. For this reasons user's passwords should be monitored.

With this operational type of monitoring in place the management of an organisation should have peace of mind that the current state of security is under control. Although top management can delegate the responsibility of security they are still accountable for it. With an efficient monitoring structure in place management can feel content that the responsibility has been delegated and will be dealt with. In the event that it is not dealt with, management will be informed and can take the appropriate action.

4 ENFORCING SECURITY CONTROLS

There are various security controls that can be put in place to secure an IT environment. One should bear in mind that while security controls help manage risks, they do not eliminate them. IT Governance Institute [10] defines controls as "the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or at least detected and corrected." Some of the more popular security controls are listed in table 1.

Table 1: Various Security Controls

Control	**Frequency of Change**
Policies	low
Organisational design	low
Operating procedures	low
Technical controls	medium -high

As portrayed in table 1 each control has a different frequency of change. Policies for instance change fairly infrequently. Technical controls on the other hand change much more frequently. The different controls are discussed in turn briefly.

4.1 Policies

There are various types of policies that an IT department can enforce, including security policies. Security policies are a set of rules that must be observed, and are published and communicated to employees, customers and vendors [12]. Security policies are not optional, they must be obeyed. For example, if a policy specifies that employees are forbidden from installing their own software onto a company computer, and the employee does so, he or she is in direct violation of the policy. Policies are not restricted to security policies, and an organisation can have various policies in place to govern its IT infrastructure. An Acceptable User Behavior Policy and an Internet Usage Policy are two other common policies that organisations make use of.

4.2 Organisational Design

Organisational design is another type of control that companies can utilise. The design covers issues such as an auditing department's line of reporting. It is a well-accepted business rule that auditors should act independently [4]. This suggests that auditors should not be able to audit their own or related work. An auditor should be external or come from a separate department.

4.3 Operating Procedures

Organisations can put various operating procedures in place to ensure security. An example of this is Separation of Duty (SoD). SoD attempts to reduce the likelihood of collusion of employees by distributing the responsibilities for tasks in a business process between various participants [4]. The signing of cheques is a good example of this. Many organisations require two different signatures on a cheque. This is a form of SoD as one person can not perform a task on their own but needs the approval of a second person.

4.4 Technical Controls

When it comes to security there are numerous technical controls that an organisation can employ. For instance, an organisation can enforce the use of passwords to gain access to the network as a security measure. This type of control, however, is reliant on the selection of secure password by network users. Technical controls that are in use in organisations often change quite frequently. Users, for example, should change their passwords on a regular basis. If an organisation is using virus protection the virus pattern file should be updated on a regular basis to ensure continued protection.

It is a good idea to put security controls in place in an organisation. The authors, however, feel that these controls should be monitored in real-time.

5 REAL-TIME RISK MONITORING

It should now be evident from the content of this article that the authors support the effective securing of IT systems from threats, and the use of risk management in order to ascertain how much to secure an IT environment and whether the expenditure can be justified. The authors now propose the use of a digital dashboard as a means of continually monitoring an organisation's risk in real-time.

Sound business decisions are based on timely, relevant and concise information [9]. This can be provided for time-pressed security personnel and managers by making use of dashboard technology. In this way management can make informed decisions as and when the need arises. A digital dashboard is a specialised portal that consolidates dispersed information into one place [14]. In this way dashboards assist organisations by reducing the effort and the time that is needed to locate and manage information from many different sources.

The higher levels of security controls, such as policies, organisational design and operating procedures change fairly infrequently. The technical controls, as discussed in the previous section, change on a more regular basis. For this reason the technical controls should be monitored. Access control, for instance, is an example of a security control that is well suited to monitoring in a real-time manner. In this way security personnel can be alerted as and when an access violation is in progress. The digital dashboard is proposed as it makes no sense to be alerted after the violation. One wants to prevent the access in order to minimise the possibility of loss of confidentiality or data integrity.

Digital dashboards have been used successfully in many different environments. For instance Deloitte and Touche, which is a professional services firm that employs in excess of 90,000 people and is situated in 130 different countries, has made successful use of dashboard technologies. The Deloitte and Touche mission statement is: "To be the professional services firm that consistently exceeds the expectations of our customers and our people." In order to live up to its mission Deloitte and Touche wanted to give their practitioners easy access to current information that was needed to exceed their clients' expectations [13]. They achieved this by providing a digital dashboard for their practitioners, which allows information to be pushed to the practitioners, preventing them from having to look for it.

There are many security controls that could be monitored in a real-time manner. The dashboard could regularly test for weak user passwords for example or it could

search for open ports on the network. Please note that in both of these situations the word monitor is used and not the word logged.

5.1 Risk Monitoring vs Logging

At this stage it is a good time to differentiate between monitoring and logging. Although the terms are often used interchangeably they actually provide very different purposes [12, p. 327]. Monitoring systems are put in place to track and fix incidents as they occur. Logging, on the other hand, provides historical information. The one provides an instant snapshot, the other provides historical records. Security risks should be monitored 24x7. Even when security staff are not on site, alerts can be sent to a pager or a cellular phone. The sooner a security incident is detected, the sooner it can be contained and removed [12, p. 327]. It should be noted, however, that in many cases monitored information can be logged and used for historical purposes, although the primary role of monitored information is to provide an instant snapshot and generate any required alerts.

6 CONCLUSION

Information security is a grave concern in today's global information society. Information is an important asset, so its protection is of vital importance. Risk management can assist organisations in deciding how much to secure an IT environment and whether the expenditure will be justified by the benefit. Risk is largely the responsibility of corporate governance. The management of IT and its related risks is now being understood as an integral part of corporate governance. There are various security controls that can be put in place to secure an IT environment adequately. One should bear in mind, however, that while security controls help to manage risks they do not eliminate them.

This article has proposed the use of real-time monitoring and alerting in the form of a digital dashboard in order to stay abreast with the technical controls that an organisation might have in place for its security. The real-time information gleaned from the digital dashboard, albeit at that point summarised and not real-time anymore, could assist with strategic and tactical decisions. For instance, if the dashboard was to pickup that users frequently selected weak passwords, the decision to do some additional security training could be made.

7 ACKNOWLEDGMENTS

The financial assistance of the National Research Foundation (NRF) towards this research is hereby acknowledged. Opinion expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the National Research Foundation.

8 REFERENCES

[1] Anonymous. *Maximum Security.* Sams Publishing, 201 West 103rd St., Indiana, 46290 USA, 2003.

[2] Bank for International Settlements. Overview of The New Basel Capital Accord. Technical report, Bank for International Settlements, Available from: `http://www.bis.org/bcbs/bcbscp3.htm`, April 2003. Last cited: 18 April 2004.

[3] B. Blakley, E. McDermott, and D. Geer. Information Security is Infomation Risk Management. *Communications of the ACM*, pages 97–104, Sept. 2002.

[4] R. A. Botha. *CoSAWoE A Model for Context-sensitive Access Control in Workflow Environments.* PhD thesis, Rand Afrikaans University, Faculty of Natural Sciences, November 2001.

[5] F. Farahmand, S. B. Navathe, G. P. Sharp, and P. H. Enslow. Managing Vulnerabilities of Information Systems to Security Incidents. *Communications of the ACM*, pages 348–354, 2003.

[6] D. Geer Jr, K. S. Hoo, and A. Jaquith. Information Security: Why the Future Belongs to The Quants. *IEEE Security & Privacy*, pages 24–32, July 2003.

[7] D. Gollmann. *Computer Security.* John Wiley & Sons. Inc., 605 Third Avenue, New York, NY 10158-0012, 1999.

[8] Institute of Directors. *The King Report on Corporate Governance for South Africa - 2002.* Institute of Directors, 2nd Floor, 15 Wellington Road, Parktown, 2193, South Africa, 2002.

[9] IT Governance Institute. COBIT Control Objectives. Technical report, IT Governance Institute, Available from: `http://www.isaca.org`, July 2000. Last cited: 17 April 2004.

[10] ITGovernance Institute. COBIT Management Guidelines. Technical report, ITGovernance Institute, Available from: `http://www.isaca.org`, July 2000. Last cited: 17 April 2004.

[11] E. Kritzinger-von Solms and L. A. M. Strous. Information Security: a Corporate Governance Issue. *Integrity and Internal Control in Information Systems V*, pages 115–133, 2003.

[12] A. Liska. *The Practise of Network Security.* Prentice–Hall, Upper Saddle River, New Jersey 07458, 2003.

[13] Microsoft Corporation. Deloitte & Touche Employees Use Digital Dashboard to Drive Success and Work/Life Balance. Technical report, Microsoft Corporation, Available from: `http://www.microsoft.com/resources/casestudies/CaseStudy.asp?casestudyid=11627`, 2002. Last cited: 20 April 2004.

[14] F. C. Rice and P. Cornell. Three Ways To Create a Digital Dashboard and Add a Web Part. Technical report, Microsoft Corporation, Available from: `http://msdn.microsoft.com/library/en-us/dnoxpta/html/odc_digdash.asp`, November 2001. Last cited: 20 April 2004.

[15] G. Stoneburner, A. Goguen, and A. Feringa. Risk Management Guide for Information Technology Systems. Technical report, National Institute of Standards and Technology, Available from: `http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf`, October 2001. Last cited: 17 April 2004.

[16] United States General Accounting Office. Information Security Risk Assessment Practices of Leading Organizations. Technical report, United States General Accounting Office, Available from: `http://www.gao.gov/special.pubs/ai00033.pdf`, November 1999. Last cited: 17 April 2004.