INTERNATIONAL JOURNAL OF NATURAL AND APPLIED SCIENCES (IJNAS), VOL. 3, NOS.1& 2 (2008); P. 75 – 81. 4 TABLES

Security of networked information systems

E. E. Essien[1]

ABSTRACT

This work presents a detailed analysis of security in the context of information systems. The role that the network plays in the overall security of the information system is discussed; as well as the gradual shift of focus of information technology (IT) managers into security issues as the internet began to proliferate during the mid -1990s. This is followed by a discussion of the IT control requirements identified by Gartner Research, and a description of the various information security standards being used around the world. It concludes with a discussion of the roles that policies and the people play in the security of Information Systems in an organization.

INTRODUCTION

The need to accommodate more complex business transactions over networks is changing the future of information security models (Fonseca and Lee, 2001). Security of an information system was considered to be a technical issue to be handled by the IT department until recently. But Fonseca and Lee (2001) report that with the increased interaction between security and e-commerce, the line separating business and IT departments is continuing to blur. Lindstrom, cited by Fonseca and Lee (2001), states that it is not just security folks that go to [security conferences] anymore; it is e-business directors and chief information officers (CIOs) of pure-play businesses that want to be up to speed [about] what infrastructures are doing security-wise.. A Gartner Group report (Witty, 2001) also re-emphasises this notion. The Gartner report estimates that about 90% of the current security spending is IT-related; however, it was forecasted that the non-IT portion would go up from current 10% to 40% by 2004; and has now gone beyond that. Although business or non-IT components are playing an increasingly prominent role in the security model of an organization, the need to authenticate and validate users is one of the top components of an information security model. PKI (Public Key Infrastructure) is one of the most important components of user authentication and validation.

Most security comes with controls, and DO's and DON'Ts. But it is important to identify the right balance of security measures and controls such that the right people access the right information at the right time. However, Lewis (2000) points out that achieving that balance is a challenge given the simple dynamics of e-business, when a system is required to service hundreds of thousands of end-users with potentially diverse computer platforms and requirements. Network information systems are systems exposed to global communication through e-commerce and general interaction.

There is therefore bound to exist certain amount of risks in sharing resources in this context. This research therefore examines the risk involved and the process of securing data in network information system

SECURITY AND CONTROL REQUIREMENTS

Risk and Security

Technically, risk is the probability associated with losses or (failure) of a system multiplied by the dollar loss if the risk is realized (Straub and Welke, 1998). By this definition, it is evident that risks are subjective. It is up to the management to assess risks and to classify them based on their severity. The economic aspect of managing risks also plays a role in it, because, sometimes the benefits from mitigating a risk may not justify the costs involved. At the same time, chances of occurrence of some risks may be less than the others. In general, Straub and Welke's definition of risk can be used as a simple gauge of measurement.

Role of network in security of information systems

A clear indication that security was not perceived to be a serious issue before the advent of the Internet can be seen in the results of a 1994-1995 Delphi study conducted by Society for Information Management (SIM) in the United States on the Key Issues in Information Systems Management. In the survey, SIM institutional and board members were asked to consider what they felt were the most critical issues facing Information Systems executives over the next 3 to 5 years, and they found security to be of markedly lower priority, that they decided to drop it from the list of issues (Brancheau, et al., 1996).

However, it is interesting to observe that another study was conducted in Australia around the same time specifically on security issues (Fink, 1995), probably because security was considered to be a significant issue in that part of the world.

Manuscript received by the Editor August. 13, 2007; revised manuscript accepted December 20, 2007.
[1]Department of Mathematics/Statistics and Computer Science, University of Calabar, Calabar, Nigeria
essieneyo@gmail.com, essieneyo@in.com

A convincing explanation for this inconsistency in Information Systems(IS) executives. perceptions can be found in another study (Watson, et al., 1997). Watson and his team compare and contrast the findings of 10 information systems management studies in 10 countries, and the SIM Delphi study (Brancheau, et al. 1996) mentioned above. They discovered that the possible reasons for these differences are cultural, economic development,
political/legal environment, and technological status of these nations.

Coming back to the point, the Australian Delphi study (Fink, 1995) mentioned above was conducted to identify key IS security issues by surveying IS managers of the 198 largest companies operating in the Australian Stock Exchange. The results of this study provided a ranking of IS security issues in terms of their perceived importance in the middle 1990s, as shown in Table 1.

Table 1. Top five IS security issues of the mid- 1990s (Fink, 1995:46)

Rank	Description
1	Access Control: Controls need to be devised to limit access to resources of a system only to authorized persons, as the move to open systems architecture has made this a complex task.
2	Disaster Recovery: Organizations need to identify potential threats and have procedures in place to overcome disasters, should they occur.
3	Networks: Knowledge needs to be gained on the complex security requirements of networks.
4	Security Management: Deliberate management action should be taken to reduce the organization's vulnerability to disasters, errors, and crime
5	Security Awareness: IS managers should consider using marketing methods to raise awareness of security issues.

A quick look at the results of the Top Five IS security issues of the mid 1990s clearly indicate that the IS executives were beginning to get concerned about the security issues of open architecture and networks that would become the Internet, and an organization's vulnerability to errors and crime that would become so commonplace by the end of 1990s. It is to be noted that there were only about 9 million Internet hosts by the end of 1995, whereas the number of Internet hosts today stands well over 100 million (ISC, 2000).

The open nature of the Internet provides an ever-growing list of vulnerabilities that every enterprise needs to address. As companies move a greater percentage of their revenues to Internet/e-business channels, the degree of security risks increases, and the number of controls implemented rises.

The Gartner Group estimates (Witty, et al., 2001) that in 1999, 75% of all enterprises were Internet-isolated. But by 2004, they predict that 80% of enterprises will be using the Internet as an integral part of their business processes. In other words, this finding means that security risks of using the Internet will be faced by 80% of all enterprises. It was seen earlier that 85% to 90% of all businesses on the Internet reported some form of security incident in 2000 (CSI, 2001, Fogarty, 2001; Gaudin, 2001; Veysey, 2001).

This finding reveals a potentially dangerous situation. To illustrate a scenario, consider that there are 100,000 enterprises in Singapore and Australia. Out of that, by 2004:

- 80,000 of them will use the Internet for critical business processes.
- 72,000 of them will experience some security incident (based on 2000 data).

In other words, approximately 72% or more of all businesses in Singapore and Australia are under threat of security risks from the Internet alone, unless adequate measures are been taken.

IT control requirements

As vulnerabilities and risks associated with information systems increase, corporations are faced with an ever-longer list of controls to be implemented to protect their businesses.

The seven IT control requirements needed to adequately and comprehensively protect an enterprise are defined as authentication, authorization, confidentiality, integrity, privacy, non-repudiation and availability. The Gartner Group identifies (Witty, et al., 2001) an eighth requirement titled .Non-interference that addresses someone trespassing within an enterprise, which, for example, may be used as a launch pad to another enterprise.

Security of networked information systems

Table 2 below describes the eight IT control requirements and possible security control tools currently available for each of them.

Table 2. IT control requirements (source: Gartner research Witty, et al., 2001:1-25)

Requirement	Definition Security	Control
Non-Interference	Ensure that control is exercised over the entry and use of an enterprise's electronic assets.	• User ID/Password • Firewall • Nondisclosure of Passwords
Authentication	Ensuring that users and applications are appropriately identified before gaining access to information assets.	• User ID/Password • Token • Biometrics Device • PKI Credentials
Authorization	Ensuring that a properly authenticated user/application can access only those IT resources to which the information owner has given approval.	• Access Control List • Attribute Certificates
Confidentiality	Ensure that only those people who have a need to see information are able to see it.	• Encryption
Integrity	Ensure that it can be identified if a transaction has changed between the sender and the receiver.	• Message Authentication Code (MAC)/Hash
Privacy	Ensuring that information provided by employees, customers and others is protected so that the information is used solely for the stated purposes of the enterprise's customer privacy policies, the person has authorized such use and its use is in compliance with all local privacy regulations.	• Policies & Procedures • Encryption • Policy Management Tools
Non-Repudiation	Ensure that both the sender and receiver of information can unequivocally prove that the exchange occurred.	• Digital Signature • Time Stamp
Availability	Ensure that an enterprise's IT infrastructure has suitable recoverability and protection from system failures, natural disasters or malicious attacks.	• Redundancy • Load Balancing • Policies & Procedures • Business Continuity • Plan • Alternate Processing • Site

INFORMATION SECURITY STANDARDS

As seen earlier, Information Security has been a pressing problem around the world. This situation has resulted in various standards being used around the world (AusCERT, 2000). These Standards set forth methods and guidelines for tackling the security issue. Some of the standards related to Information Security are listed in Table 3. The approach used for this project is based on Australian Standard AS/NZS 4360.

Table 3. Information security standards

Standard	Description
AS/NZS 4444	This two-part standard is the primary information security standard being used in Australia and New Zealand. This has two parts: code of practice for Information Security Management, and Specification for Information Security Management Systems.
RFC 2196	The Internet Engineering Task Force (IETF) has produced this standard, known as the .Site Security Handbook,. which provides practical guidance to administrators trying to secure their information and systems services.
BS 7799	This is a widely accepted British standard, which is the basis for Australian Standard AS/NZS 4444.
ISO 15408	The International Organization for Standardization (ISO) has produced ISO standard IS 15408. This standard is widely known as "The Common Criteria for Information Technology Security Evaluation v2.1 (ISO IS 15408)."
AS 4539	AS 4539, Information technology - Public Key Authentication Framework, is the Australian Standard that governs Public Key authentication frameworks.
AS/NZS 4360	AS/NZS 4360 is the most widely used standard for Risk Management. The Joint Standards Committee created this Standard, and this is considered to be world.s first Risk Management Standard.
HB 231:2000	This is the Australian Standards guideline for Information Security Risk Management, which is based on Standard AS/NZS 4360.

Security principles from the industry leaders

Many people believe that the Big Five Accounting and Consulting firms are particularly strong in Enterprise Risk Management services. Most of these firms have been around for several decades. The tools and methodologies they use are tried and tested on thousands of clients around the world. For example Deloitte & Touche, more than a century-old company, has over 73,000 consultants working in 132 countries around the globe.

As the Internet became popular and enterprises began depending on it for critical business transactions, most of the Big Five firms also ventured into e-Security risk assessment and management arena, armed with their experience of dealing with risks in the traditional setting.

Deloitte & Touche is one of the prominent players in Enterprise Risk Management services today, along with PricewaterhouseCoopers, Ernst & Young Cap Gemini, KPMG and Andersen. Deloitte & Touche and Ernst & Young are remarkably strong in Internet security arena. Deloitte even runs a .computer forensic lab. in San Francisco, which is specializing in the investigation of corporate computer crimes and fraud. The following are the components of Deloitte's guiding security principles for the design of information security architectures, which are particularly relevant to the case being assessed in this work:

- **Intrusion:** Ensuring that access to systems and information can only be gained though authorized access methods.
- **Authentication:** Ensuring that only authorized personnel are able to access the systems and information.
- **Authorization:** Ensuring that access to systems and information is restricted to those with an authorized requirement for such access.
- **Encryption:** Protecting information in transit and in storage through the use of encryption.
- **Accountability:** Ensuring that access to systems and information by users is appropriately recorded.
- **Availability:** Ensuring that systems and information are available to authorized users whenever required.
- **Endurability:** Ensuring that security risks are maintained at acceptable levels over time.

Security policies

Imposing network and systems security is only a part of the overall security strategy. The literature refers to the policies as another important aspect of security. As seen earlier (Lewis, 2000), a critical component of managing risk is to assign and manage liability clearly. Lewis points out that authentication systems allow organizations to assign liability to an account, and the person owns that account. Such dependencies can be articulated in the security policies of the organization. Lewis suggests that security policies can also explicitly define what people can do and when they can do it, and policy conditions under which they are operating, assigning, sharing or disclaiming any liability associated with their actions. Non-repudiation, or the use of logging and auditing functions to prove that something actually happened, can also be used as tool in the case of an incident. Usage of insurance instruments is also proposed as part of the policy measures to indemnify businesses (Lewis, 2000). The author observes that the insurance industry is coming up with a completely new set of instruments targeted at this area.

In addition to this, to effectively deal with system and security risks, Straub and Welke (1998) propose that managers should initiate a theory-based security program that includes

(1) use of a security risk planning model,

(2) education in security awareness, and

(3) countermeasures matrix analysis.

Perhaps the most important aspect is defining and imposing an acceptable security policy framework for the organization as far as usage of information systems is concerned. It has been observed that insider attacks, or attacks from the employees, attribute to a major proportion of network attacks (Ehinger, 2000). Ehinger observes that effective implementation of network resources use policies could prevent such events to an extent. Examples include policies on using modems in the corporate networks, telecommuting, and usage of Email and the Internet.

People and security risks

The people aspect of systems security is an area not to be overlooked. Long (2001) stresses the importance of background checks of people before employing them and assigning them to work on critical information systems. Long points out that lowering applicant screening standards may result in putting the wrong person on the payroll and open the road to work-related crime and related issues.

Some researchers believe in the importance of ethical issues associated with accessing and using confidential information (Smith, et al., 1996; Kreie and Cronan, 2000). Today's information technology makes vast amount of information accessible to businesses and their employees. The authors point out that this creates the potential for misuse of information technology, and businesses are to be concerned about the ethical behaviour of their employees and the security of their information systems. Smith, et al. (1996) point out that information privacy has been called one of the important ethical issues of the information age. Kreie and Cronan (2000) believe that in certain situations, external influences such as company standards are likely to affect employees' behaviour. The proposed solution to this issue is to encourage ethical decision making by having a written code of ethics and providing ethical training.

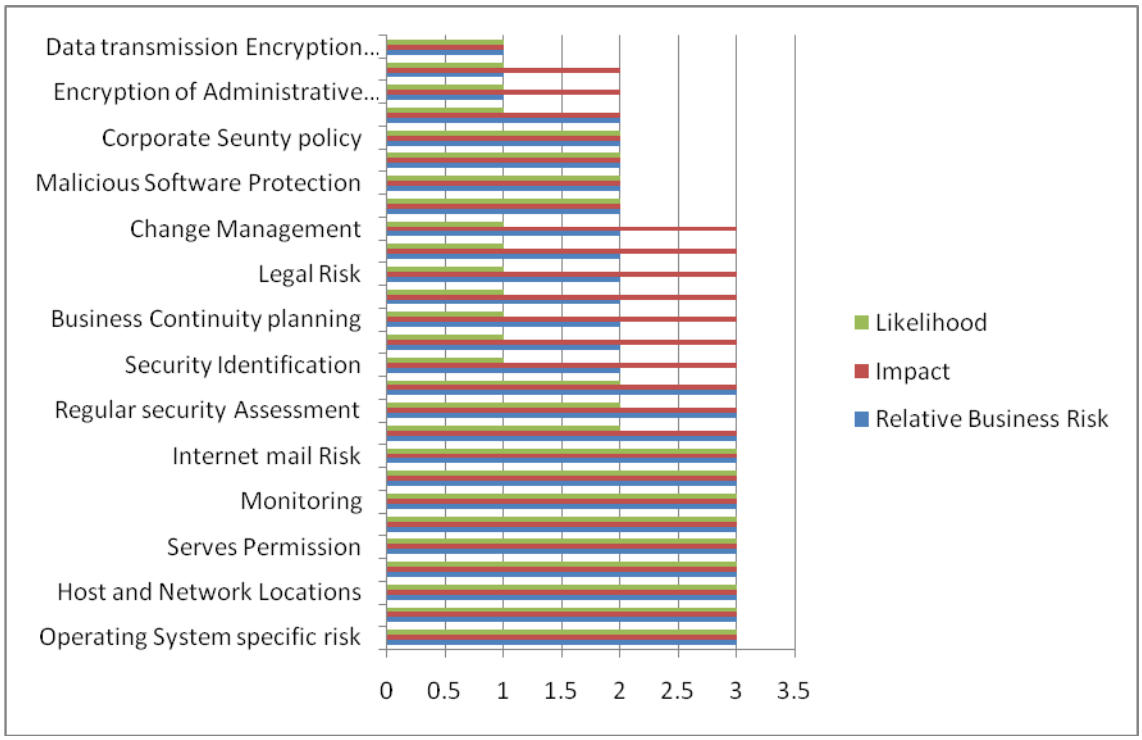

Fig 1. Assessment of security risk, impact and likelihood of occurrence

Countermeasures of risks

It is widely accepted that counter measures, or strategies adopted to reduce security risks, fall into four categories of sequential actions (Straub and Welke, 1998), namely:

(1) deterrence,

(2) prevention,

(3) detection, and

(4) recovery.

Straub and Welke notes that a certain portion of the potential system risks can be prevented by **deterrent** techniques, such as policies and guidelines for proper system use and by reminders for users to change their passwords, etc. If users choose to ignore deterrents, the next line of system defence is **preventives**, such as locks on computer room doors and password access controls. The literature refers to preventive measures as active countermeasures with inherent capabilities to enforce policy and prevent illegitimate use (Straub and Welke, 1988).

If abusers successfully penetrate through the first two levels of defence systems, the organization needs the ability to **detect** the misuse. Examples for this mechanism include activity reports and system audit trails. The primary purpose of this security response is to gather evidence to identify the abuser. Finally, an effective security program should be able to help **recover** from the harmful effects of a harmful act and to punish the offenders.

CONCLUSION

The evolution of network-based computing has caused IS managers to rethink their priorities and perceptions of risks. Studies have identified that security was not considered to be a major issue in the pre-internet era, the early 1990s. But studies conducted in the mid-1990s revealed that managers were beginning to worry about open architectures and security issues posed by networks and by the end of the 1990s, security was topping the list of major issues in IS. This change of perception eventually gave birth to various IT control requirements and industry standards that largely govern the process of security risk management today. The role of technology is paradoxical as it is the one of the primary causes of security risks. Thus familiarity with technology and being informed of the latest developments is a primary requirements for security practitioners.

REFERENCES

AnscERT (2000). Information security standards. Australian computer emergency response team. URL: http://WWW.ansert.org. au/ Information standards. Html Xi Sep 2002]

Braucheaus, J.C.. Jane B. D. and Weatherize, J.C. (1996). Key issues in information system management. 1994-1995 SM Delphi results.*MIS Quarterly, Minneapolis*, 20:152- 225.

CSI (2001). Financial losses due to internet intrusions, trade secrete theft and other cyber crimes soar. Sixths *annual computer security Institute IB computer crime and security survey*, (press release), URL: http://www.csi.com/prelea_000032.htm . Aug 2001.

Ehinger, D.P. (2000). Consideration for an acceptable use policy for a commercial enterprise. SANS Institute. URL: http://www.sans.org/infosecFAQ/policy/considerations.html [11 Sep 2001]

Fink, D. (1995). IS security Issues for the 1990s: Implications for management. *Journal of System Management*, Cleveland, 46(2) : 46.

Forgarty, K. (2001). "Better part of valor?" computerworld, 2001. *Framingham*, 16 (35): 29-38.

Fonseca, B. and Lee, S. (2001). Changing face of security, I*nfoWord*, Framingham, 23(16) : 8.

Gaudin, S. (2001). "Cost of Computer crime explodes, survey says, *Network World*,Framingham,7(18): 1.

ISC (2000). Internet domain survey: number of internet hosts.internet software consortium survey results, URL: http//www.isc.org/ds/host –count-history.html [29 Jan 2001]

Kreie, J. and Cronan, T.P.(2000). Making ethical decisions. Communications of the ACM, New York, 43(12). :66-71.

Lewis, J. (2000). Security strategy must focus on business issue of management risk. *InternetWeek*, Manhasset, 2(831): 41.

Long, J.W. (2001). Background checks step by step. *Security Management*, Arlington, 45(2):72

Smith, S.J., Milberg, S.J. and Burke S.J. (1996). Information privacy: measuring individuals concern about organizational practices. *MIS Quaterly*, Minneapolis, 20(2) :167

Straub, D.W. and Welke, R.J. (1998). Coping with system risk: security planning models for management decision making. *MIS Quaterly*, Minneapolis, 22(4):441-469.

Veysey, S. (2001). E-commerce risk abound for companies. *Business Insurance*, Chicago, 35(13):15.

Watson, R.T. , Kelly G.G., Galliaers R.D. and Bancheau, J.C. (1997). Key issues in information system management: an international perspective. *Journal of Management Information System*, Armonk, Spring, 13(4):91-115.

Witty (2001). The price of information security. *Strategy Analysis Report, Gartner Research*, 8: 11-6534.