International Journal of Computer Applications (0975 – 8887)
Volume 100– No.2, August 2014

Information Security – Evolution, Impact and Design Factors

Suganthy. A
Department of Banking Technology
School of Management
Pondicherry University

Moinak Maiti
MBA Banking Technology
Department of Banking Technology
School of Management, Pondicherry University

ABSTRACT
Securing the business critical information is the major concern that an organization is facing with the enormous growth in the internet. This paper explores the evolution of information security and the need for protecting the information from unauthorised access. This paper also explains how the information security problem increases with the development in the technology. The technological solutions for the security problem were also discussed with their current issues. This paper also suggests the design factors to be considered when developing an information security framework and presents the key issues that the researchers can focus on in this field.

Keywords
Evolution of Information security, Security protection mechanism, Security Framework, Design Issues

1. INTRODUCTION
The information flow in any business has been tremendously increased in the past few decades and with the technological advancements the management of the large volumes of data has become much easier. Technological usage has introduced a new threat to the business in maintaining the secrecy of the information. And protecting the business related information from unauthorized access; use and modification are the major issues that the business is facing today. Information security is all about providing a viable solution for these critical issues.

There exists a misconception with the use the terms, information security, information assurance and computer security. The common goals of all these interrelated fields are in providing the three major security goals: confidentiality, integrity and availability of information; however, there exists a subtle difference between them [11].

Information security is a much broader concept than technology. As the volume of data to be maintained by an organization increases substantially, the need for protecting the business critical information also increases. And with the technological advancements, processing these large data becomes possible, and in the same way as the information is widely passed in the internet, the threat to this information also increases.

When considering security to the information, the three basic components need to be addressed which includes, the technology, the process for managing the information and the people who will the stakeholder of this information. By 2020, there may be tremendous advancements in the technology which in turn can bring more security threats.

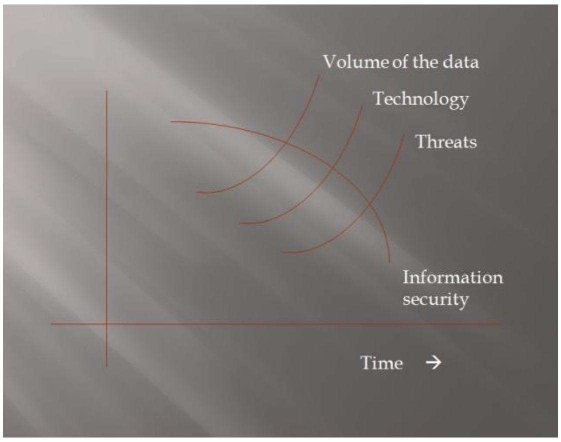

Figure 1: BOT Graph

Figure 1 shows the BOT graph which is a very powerful tool for studying the pattern of variable with an extended period of time. In the figure 1 shown above the volume of data, technology, threats and information security are four chosen variables. With the advancement of time or scientific progress in technology, volume of data also increases as result of which threats for system security like hackers, viruses, bugs, worms etc also increases. As the threat, technological advancements and the volume of the data increases, the level of security of the information decreases resulting in unauthorised access.

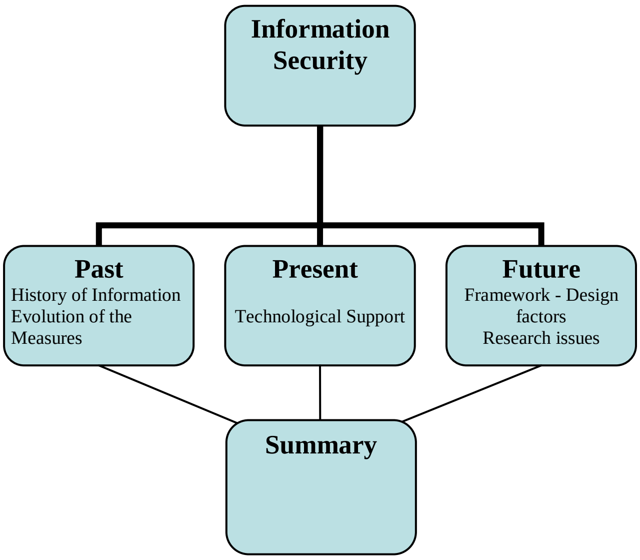

Figure 2: Framework adopted for the study

The following sections, discusses the research works carried out in the field of information security in the past, the present technological advancements and the research issues to be carried out in the future for better protection and management of the information. Figure 2 shows a framework which gives an overview of the work carried out in this paper. The framework highlights the three major divisions that are covered in this paper with respect to the Information security in the past, present and the future.

The remainder of this paper is organized as follows: section 2 gives the history of the information security focusing on the need for protecting the information and the evolution of the protection mechanisms with the advent of the technology. This section also gives the research trends of information security. Section 3 gives the technological support for protecting the information with their related issues. And section 4 gives the future trends of information security by highlighting the issues and the research areas in this field and section 5 concludes the paper.

2. HISTORY OF INFORMATION SECURITY

The most challenging issue that today's world is facing is related to security may it be of any kind. This paper is aimed to address the information security issues and to study its changing trends from time to time with the advancement in technology. This paper adopted the usage of the timeline to study the history of the evolution of information security. Timeline has been decided for breakeven with respect to the advent of the change in technology.

2.1 Need for Information Security

Before 1930: Since the existence of the human beings, people were not aware of the information or information security. They struggled to survive for their existence in search of the food, shelter and clothing which they found it as their basic needs. With the advancements, they formed groups and the need for communicating among the group members raised as a result of which the languages developed. People then started communicating orally and the information is stored only in the human memory. They then required a secondary memory for storing the information as a result of which people started using certain symbols or picture and retained the information in the rocks, but they found it was not an efficient way to store the information. People then started migrating from one place to other place for their survival, so it is not possible to take that big rocks with them. Hence, they started using metal sheets, tree leafs, clothes and at last paper to retain the information. Due to industrial revolution, there was an enormous use of paper in the Iron Age period. But during World War 1 almost all their documents were destroyed, resulting in the need for a new medium of storing and protecting the information. Till then people followed only the physical mode of storing the information.

During 1930's: Year 1930 has taken as a first breakeven point as the mode of storing information changes from physical to digital. It is the time period when computer scientists & mathematicians were working very hard to make information much more secure than before and developed the first ever Information Secured System "Enigma" (by German engineer Arthur Scherbius) which uses the techniques of encryption and decryption as a measure of security for protecting the secrecy of the messages. Which was much more compact and more secured but with the advancement in Science & technology it was first broken by the Poles (Three world-famous professors of mathematics: Stefan Mazurkiewicz, WaclawSierpinski and Stanislaw Lesniewski) in the year 1932[1]. During World War II, security threat was also raised by the British and Americans.

In 1932, the first computer Z1computer was invented by KonradZuse which was electro mechanical computer, bulkier in size, and used difficult programming languages and it is mainly used for scientific calculations, census, accounting, and payroll and inventory problems [2]. After this period there was a huge development in the field of computing. In 1942 first electronic digital computer was invented with the computing functions and parallel processing was also included in this version. In 1946 ENIAC I was developed mainly for American military research. Up to 1948 computers used vacuum tubes but after 1948 transistors were introduced and by the end of 1960 integrated circuits were invented. At this point of time information becomes much more secured than physical mode of security. This period raised a challenging question: "How one can send information from one place to another?" This leads to the thinking of networking and the year 1960 is known to be the breakeven point since this period introduced the concepts of computer networking.

During 1960: During the Cold War, Larry Roberts (the founder of the Internet) examined the feasibility of maintaining the secrecy of the United State's military's data. Finally on 3rd June, 1968 he gave the ARPANET Program Plan as shown in Table 1[3].

This was the period where the concept of computer networking, the predecessor to internet came and further improvements were done on the successive years.

1970-1990's: During this period the misuse of the ARPANET was increased due to its popularity. In December 1973, Robert M."Bob"Metcalfe [4], identified the fundamental problems with the ARPANET. And he suggested some rules and regulations for controlling the flow of information through network to make it a more secured network and also developed the Ethernet protocols. In 1979 the first worm was discovered which corrupted the files and computers. Subsequently in the year 1982 the first Apple virus was found to be attacking the Apple DOS operating system, and it spread via floppy disk followed by the first PC virus in 1986 with a threat to information security.

TABLE I ARPANET PROGRAMME PLAN [3]

Objective	Developing Networking and Resource Sharing
Technical Needs	Linking Computers
Military needs	Resource Sharing
Prior work	MIT-SDC Experiment
Effect on ARPA	Linking 17 computer research centres
Plan	Develop IMPs and starts 12/69
Cost	3.4 million dollars for 68-71

Since 1990: The period 1990 is taken as the breakeven point with the tremendous improvements in the usage of the computers by the industries. With a rapid improvement in the computer technology work of people becomes faster, accurate and easier resulting in much improvement in management sectors, finance, marketing, systems, defence etc.

2.2 Evolution of Security Protection Mechanism

Ever since the information is considered to be the most important aspect in the business, the need for protecting the information became much serious. Table 2 gives the security measures that were emerged over a period of time.

TABLE 2 THE RISE OF SECURITY PROTECTION MECHANISM

Period	Security Measures	Reference
1967	Password security in Time Sharing Computer Systems	Maurice Wilkes
1973	The need for multiple security mechanism raised in Military Systems	Schell, Downey and Popek [5]
1975	Digital Encryption Standard (DES)	Federal Information Processing Standards
1978	Operating System security and Automated vulnerability detection techniques	Bisbey and Hollingworth [6]
1979	Securing user identifications	Dennis Ritchie
1984	Identification of the computer security controls: physical control, management commitment, education of employees and administrative procedures	Grampp and Morris [7]
1984	Crypt command in UNIX and general file security	Reeds and Weinberger [8]
Since 1990	Included the concern for authenticity, availability & utility with the existing security triads: confidentiality, availability and integrity.	Donn B. Parker [12]

2.3 Information Security in Research

With the advent of the technological advancements, the threats to the information system increased drastically. And the research community has started focusing on their research in providing a solution for the security related issues. Our review on the current literature from IEEE and ACM databases shows that the research in this area has grown up to a greater extent to cope up with the newly arising threats to information security.

The table 3 shows the total number of publications related to information security since 1960.

The histogram shown in Figure 3 and Figure 4 depicts the increase in the number of publications in ACM and IEEE respectively. It clearly shows that there is a sharp increase in the number of publications since 1990. As the computer technology increases the threats to information security also increases. It's a challenge for the computer scientists to secure the information with the technological improvements. As the companies find a new way to protect the information system, the hackers are inventing ways to breach the security measures.

Figure 5 gives the histogram depicting the combined research publications of both IEEE and ACM. This chart shows that there is an exponential rise in the number of publications after 1960.

TABLE 3 THE NUMBER OF PUBLICATIONS IN IEEE & ACM

Year	IEEE	ACM
Before 1960	Database not available	Database not available
1960-1970	Database not available	Total number of publication 2 Magazine (1) Proceeding (1)
1970-1990	216 Publications Conferences(137) Journals(78) standards(1)	46 Publications Proceedings(22) Newsletter(13) Magazine(5) Transaction(3) Journal(3)
1990-2000	1207 Publications Conferences(995) Journals(193) standards(1) Books(18)	261 Publications Proceedings(80) Newsletter(19) Magazine(110) Transaction(27) Journal(25)
2000-2010	5742 Publications Conferences(5118) Journals(598) standards(5) Books(18) Early Access(3)	5331 Publications Proceedings(2642) Newsletter(324) Magazine(373) Transaction(224) Journal(56) Affil(3)
2010 and now	19997 Publications Publications Conferences(17655) Journals(2135) standards(33) Books(26) Early Access(144)	33220 Publications Proceedings(31362) Periodical(24996) Book(1858)

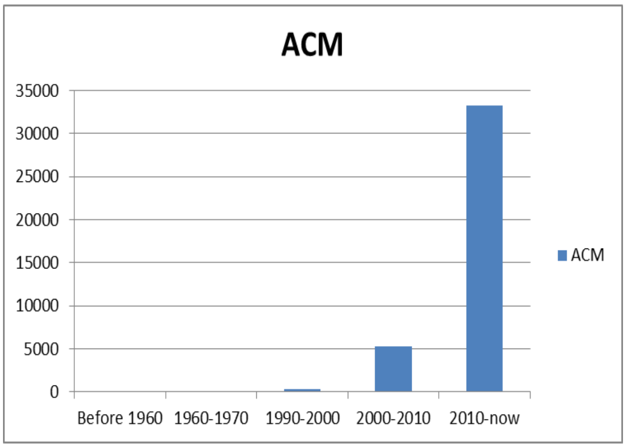

Figure 3: Histogram showing number of ACM publications

During the time period of 2000 and onwards the number of publications increases both in ACM & IEEE. In case of IEEE in the time interval 1970-1990 total number of publications was 216 and the average publication per year comes out to be 11. During the period 1990-2000 total number of IEEE publications was 1207 which is almost 6 times the publications during 1970-1990 and with a average number of 121 publications per year which seems to be the square of the previous interval and after that during 2000-2010 the publications increases to 5742 which is again 6 times more than the previous interval of time with an average publications of 575 per year. This is again 6 times more than that of the prior interval. The same trend is also seen in the case of ACM publications. Very interestingly between 2010 and 2011 within one year IEEE publication was 1515 and ACM publication was 1206 which is much more than previous intervals. This clearly indicates that researches are growing in huge number for securing the information and this seems to be an endless process.

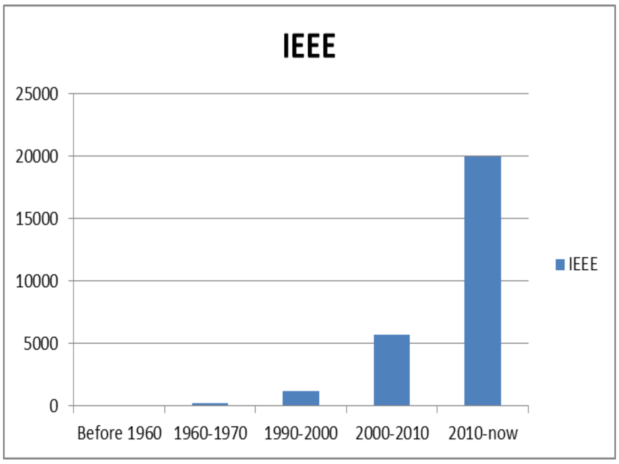

Figure 4: Histogram showing number of IEEE publications

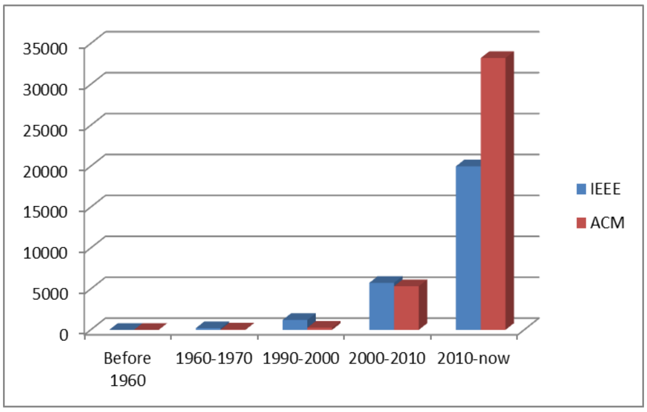

Figure 5: Combined histogram showing the number of publications in ACM and IEEE

3. TECHNOLOGICAL SUPPORT FOR INFORMATION SECURITY

Information is considered to be an important asset in today's business environment. And securing the information of a business has become increasingly more important with the ever increasing number of people connecting to the internet for various purposes.

In today's networked environment, information is not a standalone asset which can be kept in a secret place or can be kept in a locker. The information is connected with various networks and other services as depicted in Figure 6.

3.1 Security Protection Mechanism

Securing the business critical data requires lot of technological supports and since most of the business data are connected with the network either in the corporate network or in the internet, lot of issues to be considered for protecting the data from malicious users or attackers. Some of the technological solutions used for protecting the business critical data are as follows:

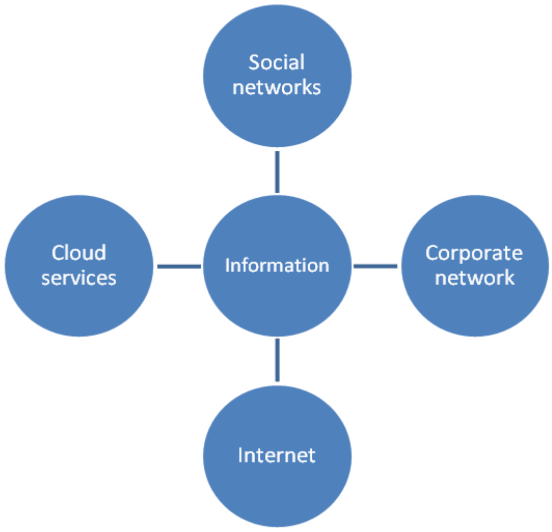

Figure 6: Information Network

Firewall: Use of Firewall has become the basic protection mechanism for protecting the corporate networks. When an organization uses firewall to protect its network, it verifies all the incoming and outgoing data. Firewall protects the unauthorized access to the corporate network. One of the critical issues related with the use of firewall is that the firewall can only protect the unauthorized access coming to the network or it protects the critical data going out of the network. If an authenticated user attacks the data it cannot be protected by the firewall. In other words, firewall is not a suitable mechanism for protecting the data when the attack is originated within the network by an authorized user.

Intrusion Detection System (IDS): IDS is an application or a device that observes the abnormal activities of a user and reports it to the administrator. The challenges with the implementation of this system are that more technical and organizational expertise is required. And what is considered to be a security violation in one network is not considered as such in another network of the same organization. So, identifying the characteristics of each network and providing the required solution is a great challenge with the use of intrusion detection systems.

Encryption Standards: Encryption is the process of converting the message to a format which can be read only the authorized people. If a hacker gets inside the corporate network and access the business critical data the data cannot be used for the hacker's intended purpose if the data is encrypted. In a business environment, encryption alone is not enough for protecting the data. Encryption can be used as a secondary level of protection mechanism.

Virus protection (Antivirus Software): The number of virus existing in today's network is astronomical. It is a critical issue in identifying the virus and providing a solution for them. And all the virus protection mechanism uses signatures in which the viruses are compared with the existing signatures and only the virus with the existing signatures are detected. And once a virus is found and its signature is included, a new virus comes in the network and this result in a great challenge for the organization to protect their network from the virus attack.

Table IV gives the security protection mechanism and their related issues.

TABLE IV Issues in Security Protection Mechanism

Technological Support	Related Issues
Firewall	Fails to detect the attack originating within the network by an authorized user
Intrusion Detection System	Requires more technical and organizational expertise
Encryption Standards	Can be used as a secondary level of protection mechanism only
Antivirus Softwares	Limited to existing signatures

3.2 Factors to be considered for designing Information Security Framework

Recent research work shows that there is a tremendous improvement in the information system protection mechanism adopted by any organizations. Every organization adopts their own framework to protect the data from the malicious attack. Data should be protected in different levels to make it more secure. And in general, the security levels to be followed for protecting the information includes protection in the data level, network level, Computer system level, application level and in the physical level.

Even after ensuring various levels of protection mechanism for protecting the data, there may be a chance of unauthenticated usage of the data. To enable a proper security a combination of more than one mechanism should be adopted.

Figure 7 gives the factors that are identified as part of this work which are considered to be more essential for designing an information security framework. The factors identified are as follows:

Figure 7: Factors to be considered for providing Information Security

Organizational need and policies: Future concerns seems to be handling the volumes of data, hence it is not necessary to make all the data to be secured but to secure only the data which are important for the organisations. Identifying the critical data is also the major issue. And it is also observed that the failure of the information system security is due to the mismatch of the organizational policy and information security policy. One of the important factors to be considered while developing an information security policy is to match the organizational policy with that of the security goals.

Threats, Vulnerabilities and Risk: Reducing the vulnerability of the system will in turn reduce the chances of attacks on the system; in turns will provide a tight information security. Identification of the risk and finding a mitigation plan will help to improve the information security to a greater extent.

Legal Ethics: Apart from building all the protection mechanisms, it is necessary to train the user of the system to utilize the resources properly. Legal and ethical concerns should be taught to the user in all the levels of the organization.

Security Goals: The major security goals of the system includes: confidentiality, integrity and availability. Every security mechanism should have a balance of all these three goals to meet the organizational requirements.

4. FUTURE TRENDS

With the increase in the use of internet and with the enormous growth of the data that an organization has to maintain there is a need for the change in the structure adopted for providing the security mechanism. This paper has identified a few unanswered questions related to information security which can be focused by the researchers in this field.

- Can Information Security give the strategic advantage to an organisation to gain competitive advantage over competitors?
- How to develop a mechanism to identify the risk associated with the critical information?

- How to develop a more secured architecture for the Information security in an organisation?
- Calculating the cost for implementing the new framework for Information security.
- Difficulties to be faced to implement the desired frame work in the existing business structure.
- Feasibility analysis of the design structure.

Finding answers for these questions are the issues that the current researchers are focusing on.

5. CONCLUSION

From this study it is noted that there is a transitive relationship between technology, information security and management. As there is advancement in the technology, there is an increase in the information security threats and consequently affecting the decision making process of the management. The existing measures of protecting the information have been analyzed and their issues were identified. This paper identified the factors to be considered for designing an information security framework.

6. REFERENCES

[1] NSA. "The Enigma". Aug 2011 from http://www.nsa.gov/public_info/press_room/2007/new_enigma_exhibit.shtml

[2] Daniel A. Wren (2005). The History of Management Thought: Wren, 5 edition In From the invisible hand to the digital hand(PP. 485); Wiley

[3] Roberts, Larry. "Program Plan for the ARPANET". Aug 2011from http://www.ziplink.net/~lroberts/SIGCOMM99_files/v3document.htm

[4] Robert M."Bob"Metcalfe[3]"Developer of Ethernet". Aug 2011 from http://web.mit.edu/invent/iow/metcalfe.html

[5] Roger R. Schell, Peter J. Downey, and Gerald J. Popek, Preliminary Notes on the Design of Secure Military Computer Systems, (Jan. 1973), http://csrc.nist.gov/publications/history/sche73.pdf

[6] Richard Bisbey II and Dennis Hollingworth, Protection Analysis: Final Report, (May 1978), ISI/SR-78-13, USC/Information Sciences Institute, Marina Del Rey,CA 90291.

[7] F. T. Grampp and R. H. Morris, "UNIX Operating System Security," AT&T Bell Laboratories Technical Journal 63, no. 8 (1984): 1649–1672.

[8] Peter Salus. "Net Insecurity: Then and Now (1969–1998)." Sane '98 http://www.nluug.nl/events/sane98/aftermath/salus.html

[9] Herbert A. Simon (1997). Administrative Behaviour" A study of decision making processes in administrative organisations". USA: The Free Press.

[10] Gareth Morgan (1980),"Paradigms, Metaphors, and Puzzle Solving in Organization Theory," Administrative Science Quarterly,Cornell University.

[11] Information security. http://en.wikipedia.org/wiki/Informationsecurity

[12] Parkerian Hexad, http://en.wikipedia.org/wiki/Parkerian_Hexad