International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue IX, September 2017- Available at www.ijraset.com

The Analysis of General Risk Management in Network Information System between the Periods of 1988-2000

P. Gnanasekaran[1], Dr. V. Umadevi[2]
[1]*Research Scholar, PG Research Dept. of Computer Science, Jairams Arts and Science College, Karur-3, Tamilnadu, India.*
[2]*Professor & Research Director, PG Research Dept. of Computer Science, Jairams Arts and Science College, Karur-3, Tamilnadu, India*

Abstract: Computer security risks are evolving overtime. Virtually every survey conducted recent times has indicated this trend of increasing security incidents. An overall introduction of Risk management is given, and two Risk Management standards are discussed: Australian Standard AS/NZS 4360:1999 and AS/NZS 4444. It is followed by an analysis of extent of Risk Management strategies: and analysis of someone of the recent computer security breaches. The security impact is difficult for one of the primary reasons. Today the whole world is discussing about the security issues hence recently NIS was attacked by Ransomware problem. Almost all the low, mid and high level organization was attacked according to their size. The present work is an approach to Exploration of Incidents and vulnerabilities, Mail messages and Internet hosts handled between the periods of 1988-2000.

Keywords: Risk Management, Security Risk, Incident, Vulnerability, Mail Message and Internet Host.

I. INTRODUCTION

In recent years increasing the interconnectivity of computers and interdependent accessibility of individuals the system are becoming insecurity. Risk evaluation of Information security plays important role not only to fix facts but also scan and note the particular incidents and vulnerabilities. Thus all the networked Information System in organizations, the information security is the challenging role [1].Technically to reduce the risks is the challenging factor.

Risk is defined as the possibilities of something happening that will have an impact upon objectives. It is measured in terms of consequences and likelyhood. Risk Management is

an interactive process consisting of well -defined steps which, taken sequence, support better decision making by contributing a greater insight into risks and their impacts [2]. Australian standards define risk management as “the culture, process and infrastructures that are directed towards the effective management of potential opportunities and adverse effects”. A risk management according to the Australian standards definition is: “The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analyzing, evaluation, treating, and monitoring and communication risk”.

The scenario of all information system risk is constructed by high level vulnerability. The low-level vulnerabilities are not causes hard hit risks and it could not produce risk factor in organizations. Each scenario are directly correspondence with vulnerabilities in One-to-one relationship and also the multiple vulnerabilities are combined and constructed a single scenario, where a single vulnerabilities can construct, one risk scenario [3].Risk assessments are used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems [3].

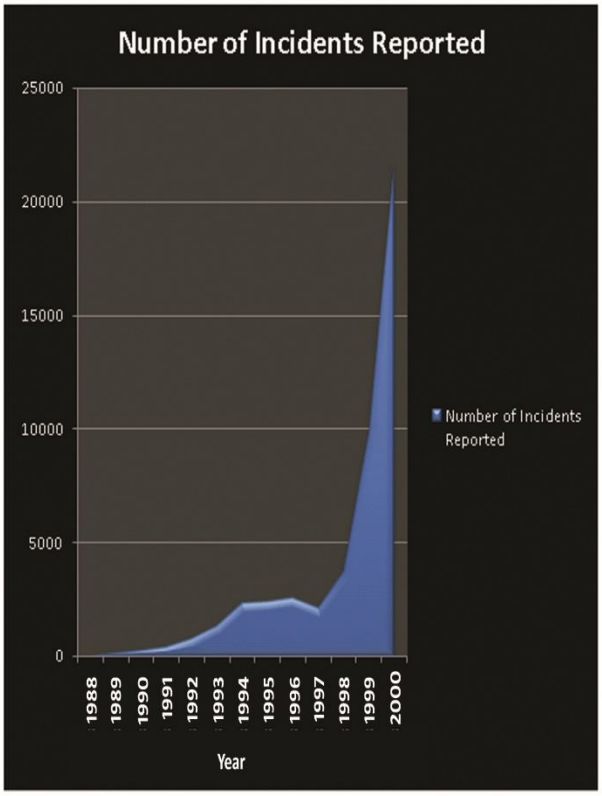
Any effort made by an organization to avoid risks and enabling the company to tackle any threats to its existence is classically called Enterprise security. We need to modify the term to include the newly conceived asset of information in this gambit so that the system would be able to protect information as well thus giving rise to an amalgamation called Information System’s Security [4]. The aim of Information System Security is to chalk out policy for security of information and to lay down procedures that would govern the handling of the informational Assets, thus achieving integrity, availability, confidentiality and authenticity of the information handled.

How has it evolved overtime?

The sixth annual 2001 Computer Crime and security survey [5] clearly illustrate this trend:
Forty percent of respondents reported outside system penetration. That number is up from 20% in 1997.
Thirty eight percent detected denial –o-service attacks. That number is up from 24% in 1998 and 27% in 2000.
In last year's survey, 249 people were able and willing to quantify financial losses. That number totaled $265 million.
Thirty six percent of respondents reported security breaches to law enforcement agencies. That is up from 17% in1997 and 255 in 2000.
Carnegie Mellon University's CERT Coordination Centre (CERT/CC) statistics illustrate the same trend. Table:1 illustrate the number of incidents reported since 1988 to 2000 [5].

Table 1: The number of incidents reported to CERT/CC Source CERT/CC Statistics

Year	Number of Incidents Reported
1988	6
1989	132
1990	252
1991	406
1992	773
1993	1334
1994	2340
1995	2412
1996	2573
1997	2134
1998	3734
1999	9859
2000	21756

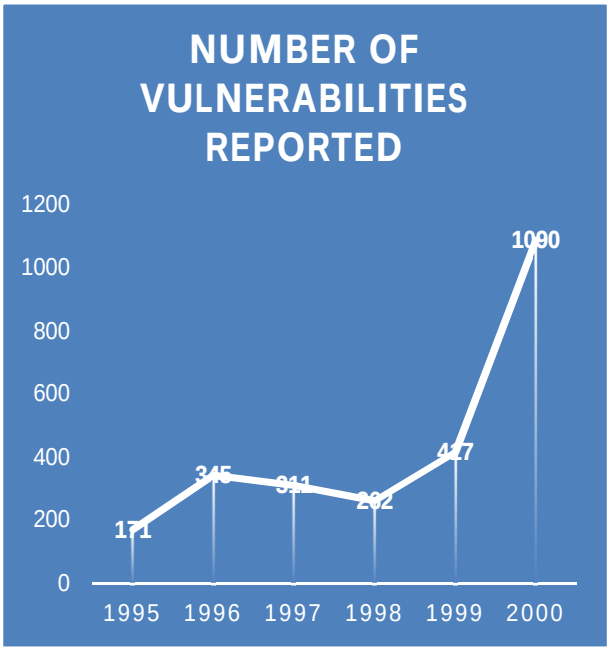


Graph 1: Number of Incidents Reported

The number of security vulnerabilities reported around the same time also shows a similar trend. Table 2 illustrates the number of security vulnerabilities reported since 1995[5].

Table 2: The number of vulnerabilities reported to CERT/CC Source CERT/CC Statistics.

Year	Number of vulnerabilities reported
1995	171
1996	345
1997	311
1998	262
1999	417
2000	1090



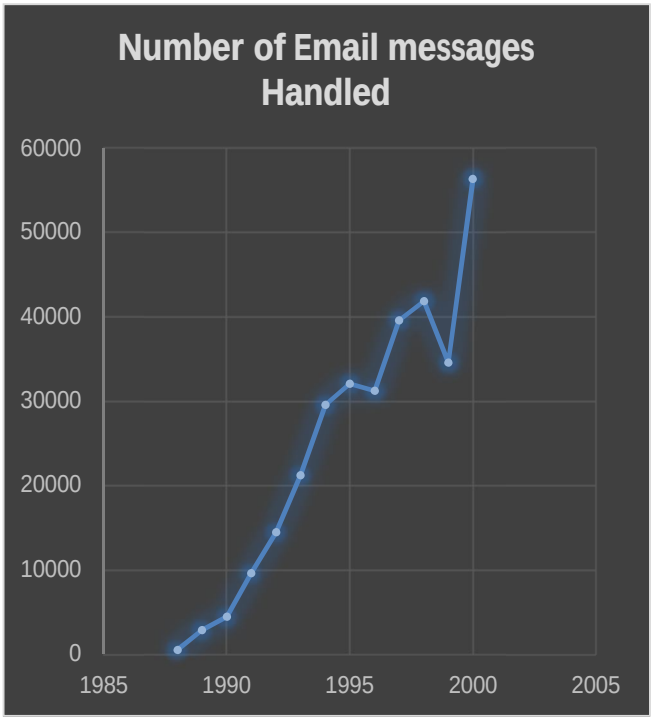
Graph 2: Number of Vulnerabilities Reported

Table 3illustrates the number of email messages handled by CERT authorities dealing with security.

Table 3: The number illustrates a significant increase in the email traffic since 1988 to 2000.

Year	Number of Email messages Handled
1988	539
1989	2869
1990	4448
1991	9629
1992	14463
1993	21267
1994	29580
1995	32084
1996	31268
1997	39626

1998	41871
1999	34612
2000	56365



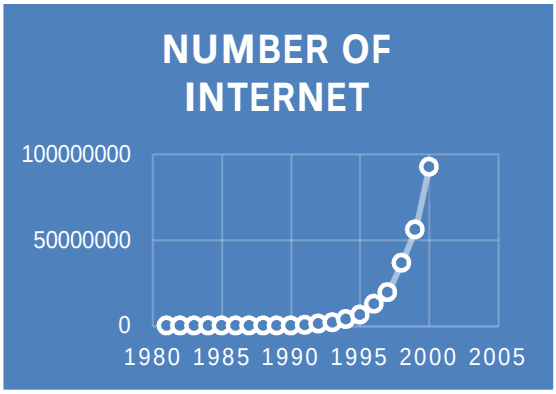
Graph 3: Number of Email Messages Handled.

The increase in the number of internet hosts shows a similar trend as well. This is a clear indication of how the security incidents are related to the growth of the Internet in general. The "hosts" or computers connected to the network make up the Internet; and the number of hosts on the network is a representation of the size of the Internet. Thus, the growth rate of the hosts is synonyms to the growth rate of the internet [6].

Table:4 Number of Internet Hosts

Year	Number of Internet
1981	213
1982	235
1983	562
1984	1024
1985	1961
1986	5089
1987	28174
1988	56000
1989	159000
1990	313000
1991	671000
1992	1136000
1993	2056000

1994	3864000
1995	6642000
1996	12881000
1997	19540000
1998	36739000
1999	56218000
2000	93047785



Graph 4: Number of Internet Hosts

II. RISK MANAGEMENT FRAME WORKS

A. Australian standard for risk management

The standard adopted for the research work is AS/NZS 4360:1999, which is the Australian/New Zealand standard for risk management. There were 2 main reasons for adapting this as the foundation for the research work. First, this standard is widely regarded as the first most comprehensive risk management standard. Secondly, The Australian organization being discussed here required a standard that was legally valid in Australia.

According the standard committee, the objective of AS/NZS 4360:1999 is to provide a generic framework for establishing the context, identification, analysis, evaluation, treatment,, communication and ongoing monitoring of risk. This standard is very generic, and independent of any industry or economic structure. The Australian standard is considered to be the world's first risk management standard.

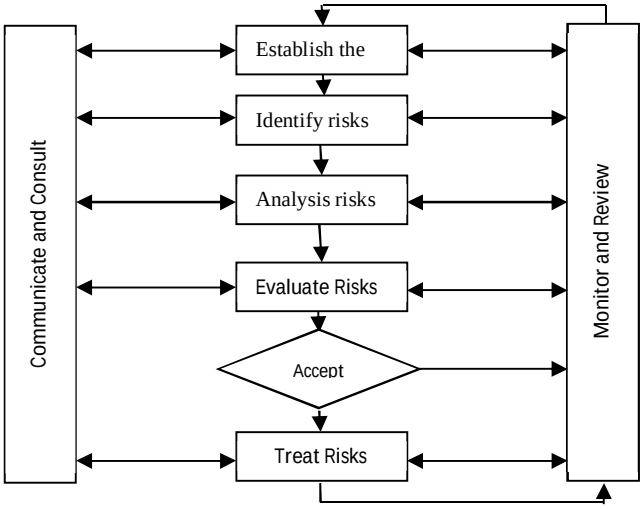


Fig:1 Risk Management Process

AS/NW 4360:1999 defines the risk management process as a multi-faced process, appropriate aspects of which are often best carried out by a multi-disciplinary team. The main elements of the risk management process are as the following

1) Establish the context
2) Identify risks
3) Analysis risks
4) Evaluate risks
5) Treat risks
6) Monitor and review; and
7) Communicate and consult

III. CONCLUSION

Nowadays, information system security is faced with some serious problems which suffer increasing threats, the increasingly complicated environment and more and more uncertain factors. But overall Risk Management is not possible while counting the number of vulnerabilities. From the statistical report of this work has make us to think about the past risk factors and their growth, and also remind us if we had taken high security phenomenon in past, the organizations would have reduced the Risk factor in Networked Information System. Hence, today the competitive business world has to focus high security standards. The Australian standard is considered to be the world's first risk management standard.

REFERENCES

[1] Xiaofong and XnTong, "A Scenario based information security risk evaluation method", International Journal of Security and its Application, Vol.B.No: 5,2014, Page:21-30.
[2] OB/7, Joint Technical committee, "Risk management: Australian/new Zealand standard, 1999.
[3] Rebecca M. Blank, US Department of Commerce, NIST,"Guide for Constructing Risk Assessments, Special publication 800-30,
[4] Daniyal M. Alghazzawi, Syed Hamid Hasan, Mohamed SalimTrigui," Information Systems Threats and Vulnerabilities", International Journal of Computer Applications (0975 – 8887) Volume 89 – No.3, March 2014.
[5] CERT/CC -2001, CERT/CC statistics 1999-2001, Carnegie Mellon University's CERT coordination Centre (CERT/CC) statics, http://www.cert.org/stats/cert_stats.html,August-2001.
[6] ISC,2000, Internet domain survey: Number of Internet hosts, Internet Software Consortium Survey Result, http://www.isc.org/ds/host-count-history.html, January 2001.
[7] OS/7,AS/NZS 4360:1995, "Risk management", Australian/New Zealand Standard,

BIOGRAPHY

P. GNANASEKARAN, is a Research scholar in PG and Research Dept. of Computer Science, Jairams Arts and Science College, Karur-3, Tamilnadu, India affiliated by Bharathidasan University, Tiruchirapalli. His areas of interest are Computer Security, Big Data, Networking, etc.

Dr. V. UMADEVI is presently working as Research Director, PG and Research Dept. of Computer Science, Jairams Arts and Science College, Karur-3, Tamilnadu, India affiliated by Bharathidasan University, Tiruchirapalli. Her research area includes Computer Networks, Computer Security, Datamining, Computer Vision, Robotics etc..