Data Security: Issues And Challenges For Disaster Management In The New Millennium

Mohd Zukime Mat Junoh, Abdullah Osman, Mohd Suberi Ab Halim, Mohd Safizal Abdullah

Abstract: Data security is a crucial issue in new millenium because the business world uses the ICT. All nations in the world may receive threat and are exposed to cybercrime from terrorists to attack their national security. Nowadays, most of organizations such as the government, the private sector and multinational company store important data for various purposes. Generally, the first step in planning the deployment of any IT system for security functionality should be a comprehensive risk analysis of the system for protection and the subsequent generation of a set of security policies. Attempting to bound the Internet from a security standpoint would have been a never ending task. However, many of the conventional risks associated with, for example, the deployment of a corporate IT communication systems may be inappropriate for global public system like the Internet. Thus, some fundamental security principles still hold for the Net and 'necessary' for data security management. This paper discusses the importance of security and how it can be integrated into this emerging market and the policy implication for data security. Finally, this paper seeks to highlight data security issues for national security and challenges in disaster management in the knowledge-based economy in the New Millennium.

Index Terms: data security, disaster management, security policy.

1 INTRODUCTION

Information Technology (IT) has become part and parcel of the business world today. In fact, it will continue becoming an even larger factor in the future. Organizations will interlink their IT systems as a result of linking to the Internet, EDI, EFTPoS, etc. All of this might hold an information security risk for an organization. Organizations attempt to secure their own IT-environment, but they have little control over the IT systems they link with. If those external IT-environments are insecure, they might pose a threat to the IT systems in the host environment. The centralised computer systems are now replaced with or connected to the distributed systems. Also, multiple servers are connected to each other on a corporate network to balance their processing power. If one of the servers in the networked environment crashes, troubles will arise for both the users and the company. As organizations link their computer networks to the Internet or to the IT networks of business partners, central control over their IT systems and users, and thus information security can be lost to a large extent. However, the information security policy, which dictates the behaviour of users within an organization, has no influence on any users outside the boundaries of the organization. To ensure a secure IT-environment, under these circumstances, will call for a secure IT community.

The growth of distributed systems and the global business environment make corporate decision makers believe that having a backup or recovery plan is necessary. Many companies need to process the mission-critical information stored in distributed or client/server systems throughout entire enterprise networks. One of the success factors for a company's business operations is based on the continuance of these enterprise networks. Client/server systems have replaced the centrally located mainframe, residing at multiple sites in a building or across a corporate WAN. Consequently, protecting these client/server systems has become a major priority for corporations today [1]. Distributed systems are becoming an architectural standard for networked organizations. These systems have diffused mission-critical data across local area networks, which extend corporate resources to remote work sites. As distributed systems continue to replace the "glass house" environment of the mainframe, the data decentralization is going to increase in the future [2].

2 DEFINING DISASTER

From an information technology (IT) point of view, a disaster is an event that creates an inability to maintain the flow of ***data*** necessary for critical operations over a prolonged period of time. This might mean that ***data*** got lost and is completely unavailable, or that it is temporarily irretrievable-preventing its access or update. According to Semer [3], possible IT disasters will include:

- natural disasters, such as fires, earthquakes, lightning, storms, and static electricity;
- software malfunctions;
- hardware or system malfunctions;
- power outages;
- computer viruses;
- man-made threats, such as vandalism, hackers, and sabotage; and
- human error, such as improper computer shutdown, spilling liquids on the computer, and cigarette ash.

Unpredictability is a hallmark of disaster. Even if we know what types of disasters are possible, there is seldom any way to anticipate which type will befall. The key, therefore, is to prepare for all types.

- *Zukime Mat Junoh currently is lecturer in School of Business Innovation & Tecnopreneurship, University Malaysia Perlis. E-mail: zukime@unimap.edu.my*
- *Abdullah Osman & Mohd Suberi Ab. Halim are currently senior lecturer in School of Business Innovation & Tecnopreneurship, University Malaysia Perlis E-mail: abdullahosman@unimap.edu.my & suberi@unimap.edu.my*
- *Mohd Safizal Abdullah currently is lecturer in School of Business Innovation & Tecnopreneurship, University Malaysia Perlis.*
  E-mail: safizal@unimap.edu.my

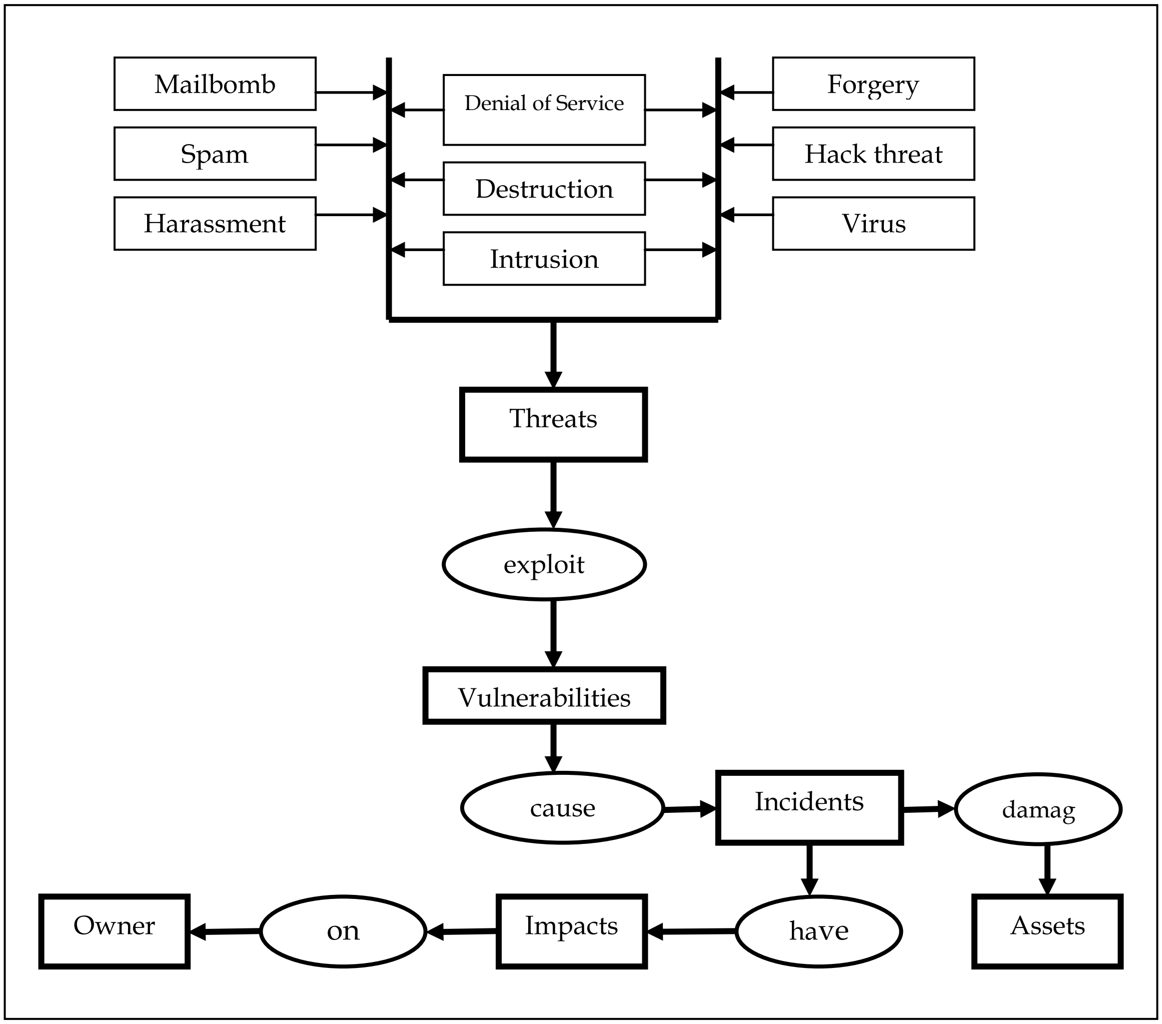

Figure 1
Threat, Asset and related concepts

According to **Figure 1** above, it showed that assets are the elements of an information system that possess a value. A security incident that will affect an asset will also have an impact on the owner of the asset (the organizations, the enterprise, or the individual). Source of threats such as virus, hackers, forgery, Spam, harassment, intrusion, denial of services, destruction and mail-bomb will exploit certain vulnerability in order to cause a security incident. Therefore, threat, vulnerabilities, and impacts should be combined together to provide a measure of the data security risk.

3 ISSUES AND CHALLENGES

Nowadays, data security has become so much of an issue in today's world because all organizations used a database to store data for any purpose and they are working within distributed environment. All organizations like government, higher education, health sector, private sector and individual must understand these issues, as vandalism or loss of ***data*** can give a negative impact on the asset, quality of services and operation management. The National ICT Security Emergency Response Center (NISER) statistics indicate that ICT security cases are expected to increase further as computer literacy rates improve. Deputy Prime Minister Dato Seri Abdullah Ahmad Badawi said "the potential and actual challenges confronting Malaysia in cyberspace are anticipated to grow in the next few decades as cyberspace expands to envelop larger areas of social, economic and political activity". According to the 2000 Computer Virus Prevalence Survey by ICSA Labs (http://www.icsalabs.com) they reported that computer virus would cost companies worldwide US$1.6 trillion (RM6.1 trillion) in damages this year. Nevertheless, computer virus outbreaks are the number one security threat to companies that have online presence (see Table 1 and Figure 2) in Malaysia. The numbers of virus and their sophistication have increased tremendously. Virus now spread in hours, not weeks. For example these virus spread through e-mail attachment, tempting users to open to them by promising "special" pictures but instead opening the attachment will activate the virus. The defence system is still a relatively preliminary stage. With the emergence of more sophisticated viruses and other types of attack, a stronger security system such as the usage of firewalls and multiple security systems is deemed necessary for greater protection. Anti virus solution are a necessity for every ICT security system and no longer a luxury.The advent of the personal computer, as well as the increasing complexity and reliability of networks, has brought about a great challenge in the area of data security:

1. The decreasing price and increasing capabilities of personal computers resulted in many people in the organization acquiring these machines.
2. The ever increasing number of software development packages available made it possible for these people to start developing their own systems
3. The knowledge gained from developing these systems could often give them the capability to circumvent security measures built into the current systems.
4. The ever increasing use of the internet meant that there were potential threats from outside the organization.

The above issues combined the fact that information systems are becoming more and more crucial to a successful daily operation of many organizations has brought about the next major advance in data security issues.

4 MALAYSIA EXPERIENCE IN ICT SECURITY THREAT

A recent study by IDC revealed that the security market in Malaysia is set to experience a time of growth. Malaysia also has experienced 1,713 ICT security cases since 1997, making that an average of 400 new cases a year (Malaysia.CNET.com: 10 April 2001). Malaysian organizations underwent a high incidence of ICT security breaches, recording a level of sixty eight percent (68 %) amongst the 205 organization survey (NISER ICT Security Report 2000/2001). The growth of increasing of ICT security incident from 1997 to 2001 and 2001 to 2013 (see Table 2) showed that Malaysia has a highly potential upheaval for data security threat.

Table 1
Threat of Data Security in Malaysia, 1997 - 2001

Types of Incident	1997	1998	1999	2000	2001
Mailbomb	29	32	18	20	5
Spam	34	146	201	156	82
Harassment	8	11	11	16	23
Forgery	4	6	17	3	10
Hack Threat	4	95	343	195	204
Virus	7	4	54	27	379
Denial of Service	5	10	10	25	19
Destruction	2	1	11	13	0
Intrusion	22	37	63	48	198
Total	**115**	**342**	**728**	**503**	**920**

(Source: Adapted from http://www.niser.org.my/statistics/)

About 92% of organizations have ICT security systems in place since year 2000. Organizations spent an average of RM120, 000 on system. This is relatively low compared to the overall IT spent of RM7.6 billion recorded in the same year [4]. The most common ICT security system in Malaysia used are such as identification authentication, antivirus solution and firewalls. According to NISER ICT Security Report 2000/2001, it is indicated that 59 % of organizations attributed the success of their security measures to antivirus solutions and 47 % to their firewall solutions.

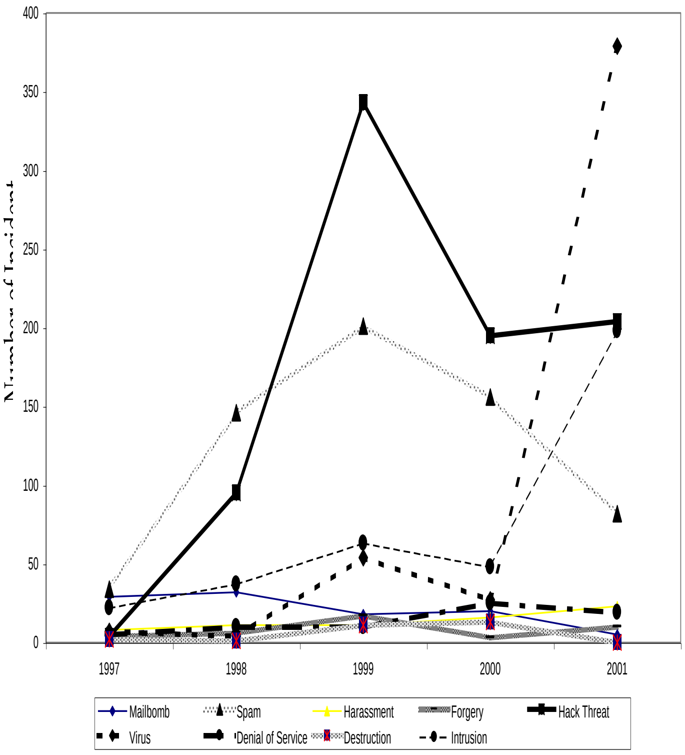

Table 2
Recent Threat of Data Security in Malaysia, 2001 – 2013

Types of Incident	2001	2005	2010	2013
Mailbomb	5	0	0	0
Content Related	0	0	39	54
Spam	82	0	1268	950
Cyber Harassment	23	43	419	512
Forgery	10	149	0	0
Hack Threat	204	87	0	0
Virus	379	0	0	0
Denial of Service	19	7	66	19
Fraud	0	0	2212	4485
Destruction	0	0	0	0
Intrusion	198	467	2160	2270
Intrusion Attempt	0	0	685	76
Malicious Code	0	82	1199	1751
Vulnerability Report	0	0	42	19
Total	**920**	**835**	**8090**	**10136**

Source: http://www.mycert.org.my/en/services/statistic/

5 CURRENT WEAKNESSES FOR DATA SECURITY

Today, most of organizations are working in LAN (local Area Network) and WAN (Wide Area Network) environment. This environment provides challenges to the security of information because of the newness of the technology and its application and lack of ownership of this problem. According to Kevin [5], he suggested that if the security of these distributed environment is to be improved, three problem areas must be tackled:

a) having effective management and control in place;
b) ensuring enterprise-wide network and platform availability;
c) preserving the viability of the data, its integrity and confidentiality.

There are three major factors of security problems in the distributed environment. These include availability issues, management and control issues and data viability issues [6] (see Figure 3).

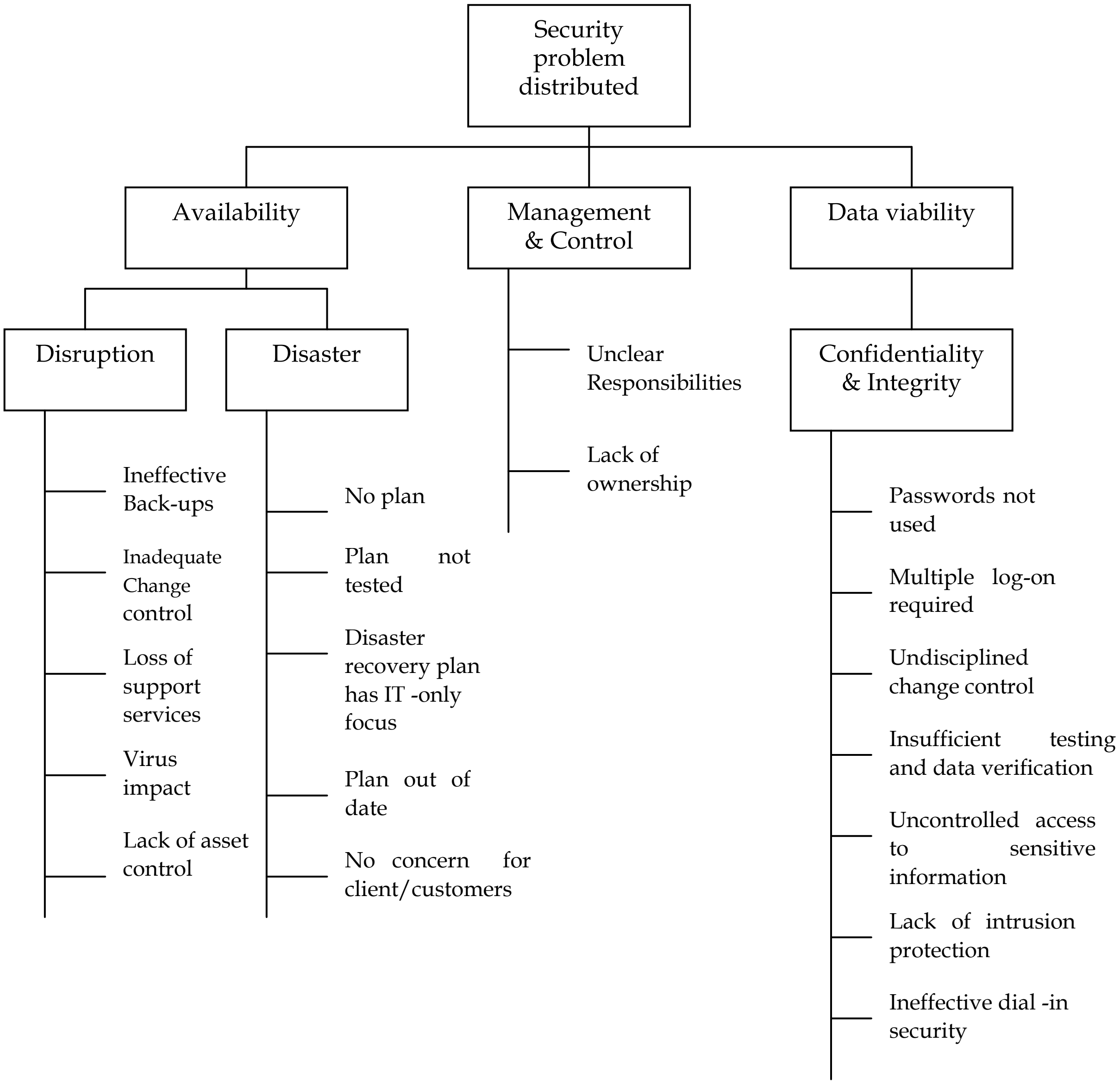
Security problem distributed
Availability
Management & Control
Data viability
Disruption
Disaster
Unclear Responsibilities
Lack of ownership
Confidentiality & Integrity
Ineffective Back-ups
Inadequate Change control
Loss of support services
Virus impact
Lack of asset control
No plan
Plan not tested
Disaster recovery plan has IT -only focus
Plan out of date
No concern for client/customers
Passwords not used
Multiple log-on required
Undisciplined change control
Insufficient testing and data verification
Uncontrolled access to sensitive information
Lack of intrusion protection
Ineffective dial -in security

Figure 3
Security problems in the distributed environment

A set of rules and regulations for all users will need to be introduced and some authorities will have to see that all parties adhere to this. There are a variety of reasons that cause systems to crash. For example, the lack of system security and employee sabotage are the main concerns. While computer hackers live outside of the company walls, this is not always the case.

RECOMMENDATION AND POLICY IMPLICATION

Ten key controls are highlighted as a fundamental building blocks for the development of data security and should be implemented first. These ten key controls are as follow[7]:

1. Information security policy document: a written policy document must be available to all employees responsible for information security.

2. Allocation of security responsibilities: responsibilities for the protection of individual assets and for carrying out specific security processes must be explicitly defined.
3. *Information security education and training*: users must be given adequate security education and technical training.
4. *Reporting of security incidents*: security incidents must be reported through the correct channels as quickly as possible.
5. *Virus control*: virus detection and prevention measures and appropriate user awareness must be implemented.
6. *Business continuity-planning process*: there must be a managed process in place for developing and maintaining business continuity plans.
7. *Control of proprietary copying*: copyright material must not be copied without the owner consent.
8. *Safeguarding of company records*: important records must be safeguarded from loss, destruction and falsification.
9. *Compliance with data protection legislation*: all applications handling personal data must comply with data-protection legislation and principles.
10. *Compliance with security policy*: systems must be regularly reviewed to ensure compliance with security policies and standards.

The main recommendations in the security policy implication of the standards are:
1. Definition of data security;
2. Statement of management intention supporting the goals and principles of data security;
3. Explanation of the specific security policies, principles, standards and compliance requirements;
4. Definition of general and specific responsibilities for all aspects of information security;
5. Explanation of the process for reporting suspected security incidents.

CONCLUSION

From the discussion above, disaster causes an event that halts the critical business functions within an organization. All organization that rely on their computer systems and networks to do their business can suddenly lose everything if their computer systems go off-line or are corrupted by a virus. In this electronic age where computers are enhancing the talents and skills of people, data are now filling the corporate offices and executive boardrooms. Hence, as computer technology and data becoming the important commodities of the future millennium, the new battle cry is 'survival of the data. As a result, data are protected from corruption and it is one of the major functions of top level management and IT professionals today. Today’s network managers work in a very complex communications environment and they must protect their networks from environmental threats and intruders. Perhaps the major security threat is made by humans, and this can be prevented with adequate security plans in conjunction with adequate programs. Constant monitoring and update of security plans to meet the corporate needs will discourage sabotage or an intentional leak of company’s critical information to outsiders. Therefore, research findings by Nik Zulkarnaen et. al., suggest that could assist ICT security professional to prepare an appropriate mitigation plan (2013) strategically for their ICT outsourcing project. Finally, organization could get optimum benefit in their ICT outsourcing strategy and simultaneously minimizing associated impacts caused by information security risks.

References

[1] Colraine, R. (1998), “Protect more, recover faster is the rule”, Computing Canada, Vol. 24 No. 30, p. 35.

[2] Mello, J.P. Jr (1996), “Taking a crack at backup”, Software Magazine, Vol. 16 No. 10, pp. 85-8.

[3] Semer, L.J. (1998), “Disaster recovery planning for thedistributed environment’, Internal Auditor, Vol. 55 No. 6, pp. 41-7

[4] Khidzir, N.Z, Mohamed, A & Arshad, N.H (2013), Journal of Industrial and Intelligent Information Vol. 1, No. 4.pp.218-222

[5] Kevin J. F. (1995), "Security and Data Integrity For LANs and

[6] WANs: The Biggest Challenge Yet to IT Security", Information Management & Computer Security, Vol. 3 No.4.pp 27-33.

[7] Steve M. H, David Y, David C. (2000), "Disaster recovery planning: a strategy for data security", Information Management & Computer Security, Vol. 8. Issue 5,pp. 1-11.