ZENITH
International Journal of Multidisciplinary Research
Vol.2 Issue 8, August 2012, ISSN 2231 5780

SECUTIRY ISSUES IN INFORMATION TECHNOLOGY

DR. S. KANCHANA RATNAM*; T.T. RAJKUMAR**

*Assistant Professor.
**Ph.D. Scholar,
Member of Madras Management of Association (MMA),
& P.G. and Research Department of Public Administration
Presidency College, Chennai - 600005.

ABSTRACT

Information systems are most vulnerable to attack by intruders, hackers, fraudsters, etc. In recent years, systems have become more susceptible to these threats because computers have become more interconnected and, thus, more interdependent and accessible to a larger number of individuals as brought out by some case studies. In addition, the number of individuals with computer skills is increasing, and intrusion, or "hacking," techniques are becoming more widely known via the Internet and other media. Numerous government reports published over the last few years indicate that governmental automated operations and electronic data are inadequately protected against these risks. These reports show that poor security programme management is one of the major underlying problems. A principal challenge many agencies face is in identifying and ranking the information security risks to their operations, which is the first step in developing and managing an effective security programme. Taking this step helps ensure that organizations identify the most significant risks and determine the most appropriate actions to mitigate them. The paper reviews information on the recent happenings involving risks in information technology and suggests methods of preventing such heinous cyber crimes. This article presents a general overview of issues relating to information security.

KEYWORDS: Computer System, Fake, Fraudsters, Hackers, Information Security, Internet, website.

INTRODUCTION

In olden times, computer system of an organization was developed, used, and maintained in isolation from other areas of business. These computer systems were centrally located and were responsible for all business operations. However, in today's modern Internet world of information browsing, the information of an organization has unwittingly become vulnerable to misuse by unauthorized individuals who has gained easy access to such classified information. When a computer system connected to the Internet is used, it is possible to reach a rich variety of sites and information. By the same token, any system connected to the Internet can be reached in some manner by any of the other computer systems connected to the Internet. Partaking of the material on the Internet also means that one has to be concerned about the security of his own computer system and that of others (Auckerman, 2002).

An organization does not want unauthorized persons accessing its information or information belonging to others who share its system. Therefore it wants to protect its system from malicious or unintentional actions that could destroy stored information or halt its system. It doesn't want others masquerading as itself. The organization needs to be concerned about the security of other systems so it can have some faith in the information it retrieves from those systems, and so it can conduct business transactions. A lack of security results in damage, theft, and what may be worse in some cases, a lack of confidence or trust. IT managers and network administrators face an increasing challenge of managing and protecting information and network resources from unauthorized access. Missing of confidential information from an organization may prove harmful for the reputation of the institution and it may loose valuable clients. To avoid such situations, organizations must secure information from misuse and damage. The term computer security is used frequently, but the content of a computer is vulnerable to few risks unless the computer is connected to other computers on a network. As the use of computer networks, especially the Internet, has become pervasive, the concept of computer security has expanded to denote issues pertaining to the networked use of computers and their resources. Some case studies are presented below to highlight the vulnerability of information at the hands of wrongdoers.

FRAUDULENT JOB OFFERS

In a recent case study of abuse of IT some fraudsters used the names of top IT firms such as TCS, Wipro, HCL Technologies, etc., and lured engineering graduates to make deposits (Vasudha Venugopal, 2012). The fraudsters under the name of 'Infinity Software Services' lured gullible students through emails offering jobs in reputed companies and asked them to deposit Rs. 5,000/- to Rs. 10,000/- as a refundable deposit in a bank account provided by them. Everything was carried out in an unsuspicious manner. Later on it was turned to be dysfunctional.

US CYBER SECURITY RESEARCH LAB HACKED

The Oak Ridge National Laboratory was forced to disconnect Internet access for workers after the federal facility was hacked, and administrators discovered data being siphoned from a server. The lab's science and technology research includes work on nuclear nonproliferation and isotope production. The lab, ironically, also does cyber security research focusing on, among other things, researching malware and vulnerabilities in software and hardware as well as phishing attacks. "One of our core competencies at the lab is cyber security research," Zacharia, deputy director of the lab, said. The attacker used an Internet Explorer zero-day vulnerability that Microsoft patched on April 12, 2011 to breach the lab's network. The vulnerability, described as a critical remote-code execution vulnerability, allows an attacker to install malware on a user's machine if he or she visits a malicious web site (Guido, 2011).

According to Zacharia, the intrusion came in the form of a spear-phishing email sent to lab employees on April 7, 2011. The e-mail, purportedly sent from the human resources department, discussed employee benefits and included a link to a malicious web page, where malware exploited the IE vulnerability to download additional code to users' machines. The attackers cast

their net wide in the company, but hooked only two computers in the phishing scheme, Zacharia said. About 530 employees received the e-mail — out of about 5,000 workers — but only 57 people clicked on the malicious link in the correspondence. Out of this, only two machines got infected with the malware

ABN-AMRO LOOSES 5.6 MILLION EURO IN CYBER THEFT

Cybercriminals have lifted 5.6 million Euro from Dutch bank ABN-AMRO. This has been reported by the Dutch police and the Dutch paper Telegraaf (both links contain Dutch language references). Their actions did not involve cooperation from bank employees. Bank officials state that this was the first time that money was stolen in a digital form from the bank without inside cooperation. Apparently the robbery already dates from March 2010, but has been made public after a 26 year old was apprehended by the Dutch police. According to the Telegraaf, this person transferred the money from his account to foreign accounts particularly in Belgium and Hungary. Currently, the affair takes on a certain proportion as in total 13 persons, between the ages of 26 and 62 years have been arrested by Dutch police (Bisaerts, 2010**)**.

FAKE WEBSITE AND FAKE EMPLOYMENT

Two engineering graduates created a website that resembled the original website of an information technology company at an Internet browsing centre where they gave false identity particulars. A security guard of the genuine company provided the duo the database of job applicants. The duo asked a few candidates to appear for an interview. They used a prepaid SIM card that had a fake address. When three candidates responded, the accused asked a few questions and said that the outcome of the interview would be communicated online. A couple of days later, the three received e-mails which stated that they had been selected for the job and they had to deposit Rs. 30,000 in the company's account. Believing this, the trio deposited money in the account of a nationalized bank which was actually that of a person in Assam. The duo had stolen his debit card for transacting through ATM located in remote areas. Like this the duo had cheated to the tune of Rs. 2.4 lakh. The police have stated that the method adopted was new (Vijay Kumar, 2010).

LESSONS LEARNT FROM THE CASE STUDIES

All these above case studies have highlighted the vulnerability of information to be stolen by unscrupulous elements for furthering their own interest thus causing serious damages and loses to governments, organizations and individuals.

INFORMATION SECURITY

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them. These differences lie primarily in the approach to the

subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer. Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas for specialization including: securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, etc.

CONCLUDING REMARKS

Information Technology and Internet have come to stay here in all walks of our life. They have become indispensable in this modern age for various business activities of an organization. They have unwittingly exposed the confidential information of these organizations to hackers and antisocial elements. The governments, organizations and public at large all over the world have become vulnerable to very high level of risks because of more and more dependence on IT and Internet. The numbers of cyber crimes as discussed above have increased phenomenally worldwide. This is the result of wide spread use of Internet and communication facilities. As the hardware and software involved in the equipments are relatively simple which could be handled easily by persons with criminal intent who could put this for wrong purposes thus causing damages and loses to organizations and individuals. The research, therefore, intends to identify various risks associated with information security and to develop a model to deal with such risks and to make the information security tamper-proof.

REFERENCES

Ackermann, E., (2002), “Legal Issues, Ethical Issues, Privacy, and Security,” Webliminal.com Production, Legal Issues, Ethical Issues, Privacy, and Security.mht.

Bisaerts, D., (2010), "ABN-Amro Looses 5.6 million Euro in Cyber theft," Information Security News, Wednesday, 22 December.

Vasudha Venugopal, (2012), "Engineering Graduates Falling Prey to Fraudulent Job Offers," The Hindu, Chennai, Vol. 135, No. 70, Thursday, March 22, pp. 6.

Vijay Kumar, S., (2010) , "Two Engineering Graduates Held for Fraud," The Hindu, Vol. 133, No. 32, February 8.