ACADEMICIA
An International Multidisciplinary Research Journal
(Double Blind Refereed & Peer Reviewed Journal)

DOI: 10.5958/2249-7137.2021.01389.6

IT AND INFORMATION SECURITY

Dr. S. Kanchana Ratnam*; T.T. Rajkumar**

*Asst. Professor,
INDIA
Email id: kanchanaravindran@gmail.com,

**Ph.D. Scholar,
Member of Madras Management of Association (MMA),
INDIA
Email id: tsqraj@yahoo.com;

ABSTRACT

Internet has come to stay in all activities of most of the people who carry out transactions such as reservation for journey, payment of bills, bank transactions, medical prescriptions and so on and so forth in their everyday life. Such activities involve handling of storage and retrieval of information. When computers became popular in public use, the devices were of standalone nature. Therefore there was no problem for individuals or organisations in ensuring the security of information stored in the computers. However, with the connectivity of computers with outside world through Internet the information held privately in computer became accessible to unknown persons who could play mischief by hacking, phising, etc. That is, information stored in computers fallen prey to unscrupulous and unauthorised persons for manipulations by them. Sometime ago, strangers entered the house of a owner of private company running the business of employment exchange at mid of night, opened his computer and attempted to steal the data of prospective candidates who had applied for job. On hearing the commotion the owner woke up and the thieves ran away. The number of such cyber crimes have increased recently thus putting at grave risk the business of corporations. Of late, there have been a large number of cases of abuse of computer information. In this modern age of widespread internet use for various business activities of an organization, it has unwittingly exposed the confidential information of these organizations to hackers and antisocial elements. This has endangered the security of information of the organizations to very high level of risks. Classified information at the hands of anti-social elements could jeopardize the security of the country too. Information Security

(IS) is the most important aspect of IT and its risk management helps the organizations to identify and manage the potential risks associated with information and information technology in a cost-effective way.

KEYWORDS: *Widespread, Anti-Social, Jeopardize, Unwittingly*

INTRODUCTION

In human life information plays a key role. An organisation requires information about its employees, a doctor requires information about his patients, etc. If a person visits a new place he/she requires information about it. Therefore information and human activities are inseparable. In essence people depend on information to manage inputs, transformation processes and output (Boddy et al, 2008). With the computerisation it has become a practice to store information in soft copy forms. With the connectivity of computers within an organisation as well as outside such as intranet and Internet have come into existence and has now become a practice to exchange information between individuals and organisations. One can also gather information from different web sites available through Internet connectivity. In the present world we cannot imagine life without Internet. From bank transactions to reservation of tickets for our travel and entertainment, and from purchases of goods and commodities to payment of bills, Internet has come in handy for all of us. Internet handles stored information and retrieves it whenever required by anybody. The revolution in business caused by the Internet and its related technologies demonstrates that information systems and information technology are essential ingredients for the success of today's inter-networked business enterprise. Information technology can help all kinds of businesses improve efficiency and effectiveness of business processes, managerial decision making, and workgroup collaboration and thus strengthen their competitive positions in a rapidly changing marketplace.

CASE STUDIES OF CYBER CRIMES

A few of the cases of cyber crimes are described below to highlight the importance of securing the information of an organisation.

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 non-proliferation 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.

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 information 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 (Guido, 2011).

Dutch Police Closes Websites from 2 Escort Agencies

Dutch police has closed 2 websites which are supposed to be related with illegal human traffic. About 1300 clients of the sites zuzana.com and pleasure-escort.nl have received an SMS from Dutch police with the message (translated from Dutch): "this phone number had a contact with the websites www.zuzana.com or www.pleasure-escort.nl. These sites offer victims of illegal human traffic. The police requests your assistance: Info: www.politie.nl/klpd/mh". Through both websites mostly Eastern European woman were offered to the clients as prostitutes for amounts of 200 Euro/hour. In the case a 32-year old male has been arrested. Another person, 37 year of age, is also wanted by French police but remains currently on the run. An international warrant has been emitted for his arrest (**Bisaerts, 2011)**.

ABN-Amro Looses 5.6 million Euro in Cyber theft

Cyber criminals 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)**.

Red Cross Fund Siphoned off Fraudulently

A former Red Cross worker Mr. Samuel Kristofer Bunner of West Virginia is accused of embezzling more than $30,000/- from its Eastern Panhandle chapter by fraudulent use of credit card. He is charged with 87 felony counts of fraudulent use of a credit card, according to an arrest warrant issued by Magistrate W. Randy Smith (Umstead, 2010). A complaint filed in magistrate court by West Virginia State Police Corporal J.M. Walker alleges Bunner "cashed out" prepaid debit cards between August 2009 and February 2010 that were supposed to be given to disaster victims.

The incidents were concealed with fictitious documentation of victims who did not exist and natural disasters that did not occur, according to court records. The alleged theft was discovered after Bunner was let go from his job, according court records.

Bunner, who was the director of emergency services for the agency, told police he worked for the Red Cross for more than three years, according to court records. When questioned, Bunner told police that he stole the money because he had a gambling problem, according to court records. "Mr. Bunner stated he would prepare a (client assistant card) authorization form under a random identity" and then sign the form, authorizing the card's activation, Walker said in his

complaint filed with the court. After activating the card, he would cash the card out, according to court records.

Most of the $30,233.71 in illicit transactions documented in Walker's complaint, are ATM cash withdrawals, with several amounting to $400 or more, according to court records. They include Martinsburg-area locations of M&T Bank, Central Bank, Susquehanna and Summit Community Bank, and 7-Eleven and Sheetz convenience stores, according to court records. Walmart stores in Spring Mills and Martinsburg, Food Lion at Old Courthouse Square and the Martinsburg Mall were among locations where debit card purchases were made with the Red Cross' money, according to court records.

Fraudulent Use of Canada Post Money Orders

Canada Post has provided the Federal Bureau of Investigation (FBI), USA with information that its Money Orders are being counterfeited and sent to unsuspecting U.S. citizens in lieu of payment for services or products purchased through the Internet, or as part of the Nigerian and other fraudulent scams. As part of the scam, the U.S. victims are instructed to cash the fraudulent Canada Post Money Order, and then send or deliver all, or part of the proceeds from the Canada Post Money Order, to the scam artists. Legitimate Canada Post Money Orders range in amounts $999.99 and less. All of the counterfeit Canada Post Money Orders, reported by Canada Post, range in amounts much larger than the $999.99 limitation, usually in the tens of thousands. The computer generated counterfeit money orders do not contain the beaver watermark on the top half of the money orders. The counterfeit money orders also contain fraudulent telephone numbers printed on the backside for verification purposes (FinCen, 2003).

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).

Stolen Emails

At Climate Summit at Copenhagen, Denmark held in 2009 several thousand files and email messages stolen from one of the world's foremost climate research institutes were circulated. This action set off a debate and led some who oppose limits on greenhouse gas emissions, and at least one influential country, Saudi Arabia, to question the scientific basis for the Copenhagen talks (Revkin and Broder, 2009).

Digits on Thumbs and Index Finger Changed

Lin Rong, a Chinese woman initially entered Japan with a fake passport and overstayed there illegally. So, she was deported to China in 2007. Now she has managed to sneak back into Japan after surgery to change the skin on her thumbs and index fingers. However, she was arrested for illegal entry. The skin patches from the digits on her right and left hands were removed and then regrafted onto the matching digits of the opposite hand. Her main objective was to fool the biometric security system at the airport because Japan's airport security system matches the finger prints of incoming foreigners to a database of wanted criminals and past deportees. Police noticed that her fingers had unnatural scars when Lin was arrested sometime ago for faking a marriage with a Japanese man. The woman had told the police that she had paid some 100,000 yuan ($16,000) for the surgery, leading investigators to believe Chinese brokers are arranging such fingerprints changes.

Film Piracy

Samantha Tumpach, a 22-year old female film fan from Chicago, Illinois during her surprise sister's birthday celebration at a movie theatre captured for three minutes a pivotal segment of the film *The Twilight Saga: New Moon* on her video camera while taping a part of the party. On a complaint from the theatre bosses the police arrested Tumpach and put her behind bars for two days. Now she faces serious piracy charges.

VoIP Misused by Terrorists

It has now come to light that terrorists including the 26/11 attackers, increasingly use popular global VoIP (Voice over Internet Protocol) engine provided by operator Skype. In this system analog voice signals are converted to digital format, compressed into Internet Protocol packets and transmitted over NET. For this, VoIP systems employ audio codecs (programs) which encode speech as digital audio. VoIp thus turns a standard Internet connection into a way to place free calls, bypassing phone networks. Because Skype has not shared its encryption code with India, it has become difficult for the Indian Intelligence agencies are not able to intercept conversation of suspected terrorists (Chatterjee, 2009).

Fake Credit Cards

Central Crime Branch (CCB) of the city police has launched a hunt for the kingpin of a gang whose members acquired credit/debit card details of customers of some petrol bunks in the city and used them to make fake cards (Peter, 2010). According to police, the culprits had cheated 13 motorists of over Rs. 8 lakh in four months. Sources with the CCB said the gang members who operated at three petrol bunks in Anna Nagar, Kodambakkam and Madhavaram used skimmer devices to capture the card details of those who made payment for fuel with their cards. "The culprits who worked at the concerned petrol stations used compact skimmers and swiped the cards of the victims by diverting their attention or moving away from the direct eye contact of the victim," said an investigating officer. The details pertaining to the credit/debit cards of the 13 victims obtained from November 2009 using the skimmer was used to make fake cards which in turn were used by the gang members to make purchases to the tune of over Rs. 8 lakh, he added.

Following police complaints by victims, a CCB team investigated and arrested Amaresan, a Sri Lankan national working in a petrol bunk in Anna Nagar. A skimmer was also recovered from him. When questioned, he confessed to the crime and revealed that Thirumurgan, also a Sri Lankan national, was his accomplice. "Thirumurgan was the agent who used to visit Amaresan on a weekly basis to collect the data obtained by the latter using the skimmer. Amaresan used to get paid from Rs. 500 to Rs. 2,000 according to the credit value of the card whose information he had illegally obtained. The data was transferred to the kingpin who along with his aides is suspected to have made the fake credit card in Chennai," the officer said.

Goof up by BA

British Airways (BA) offered in October 2009 a $40 round trip fare which includes taxes, fees, and surcharge, from any city in the US to any destination in India. Scores of eager beaver flyers snagged the tickets in the two-hour window on October 2. Later BA said it was a systems' glitch. The airline claimed that it was actually filing for a $40 increase in fares between the US and India and somewhere down the line the plus sign got knocked off (Rajghatta, 2009).

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.

CLASSIFICATION OF SECURITY IN RESPECT OF INFORMATION

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

The type of information security classification labels selected and used will depend on the nature of the organization, with examples being:

- In the business sector, labels such as: **Public, Sensitive, Private, Confidential**.
- In the government sector, labels such as: **Unclassified**, **Sensitive But Unclassified**, **Restricted**, **Confidential**, **Secret**, **Top Secret** and their non-English equivalents.
- In cross-sectoral formations, the Traffic Light Protocol, which consists of: **White, Green, Amber** and **Red**.

All employees in the organization, as well as business partners, must be trained on the classification schemes and understand the required security controls and handling procedures for each classification. The classification of a particular information asset has been assigned should be reviewed periodically to ensure the classification is still appropriate for the information and to ensure the security controls required by the classification are in place.

CONCLUDING REMARKS

In this modern age of widespread internet use for various business activities of an organization, it has unwittingly exposed the confidential information of these organizations to hackers and antisocial elements. This has endangered the security of information of the organizations to very high level of risks. The number of cyber crimes have increased recently thus putting at grave risk the business of corporations. An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification. 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

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

Bisaerts, D., (2011), "Dutch Police Closes Websites from 2 Escort Agencies," Information Security News, Tuesday, 11 January.

Boddy, D., Boonstra, A., Kennedy, G., (2008), "Managing Information Systems: Strategy and Organisation," Pearson Education Limited, Essex, England, Third Edition.

Chatterjee, M., (2009), "Spooks Want Govt to Block Skype," The Times of India, Saturday, October 3, Vol. 2, Issue 234, pp. 1.

FinCen, (2003), "Fraudulent Use of Canada Post Money Orders," Financial Crimes of Enforcement Network, United States Department of Treasury, December 2003.

Guido, (2011), "US Cyber security Research Lab Hacked," Information Security News, Wednesday, 20 April.

Peter, P., (2010), "Crime Branch Launches Hunt for Kingpin of Credit Card Scam," The Hindu, July 31.

Rajghatta, C., (2009), "BA Goofs up, Sells $40 Round-trip tickets to India," Sunday Times, October 11, pp. 1.

Revkin, A.C. and Broder, J.M., (2009), "Leaked Emails Give Naysayers Ammo," Times Global, The Times of India, Tuesday, December 9, Vol. 2, Issue 290, pp. 11.

Umstead, M., (2010), "Former Red Cross Worker Charged with Embezzling Agency's Funds," The Herald Mail, MAY 24.

Vijay Kumar, S., (2010), "Two Engineering Graduates Held for Fraud," The Hindu, Vol. 133, No. 32, February 8, pp. 1.