UNIT 7 LEGAL RESPONSES TO TECHNOLOGICAL VULNERABILITIES

Structure

7.1 INTRODUCTION

The information and the supporting processes, the computer systems and the networks, used for provision of services by an organization or for the running of the organization are crucial assets of the organization or the individual using the information systems. The confidentiality, integrity and availability of information is essential for any organization to maintain its competitive edge, cash-flow, profitability, legal compliance and commercial image. It is imperative for each organization to put in place adequate security controls to ensure data accessibility to all the authorized users, data inaccessibility to all the unauthorized users, and maintenance of data integrity and implementation of safeguards against all security threats to guarantee information and information systems security across the organization.

Information systems and the networks of the organization are increasingly facing security threats from a wide range of sources including computer-assisted fraud, espionage, sabotage, vandalism etc. The sources of damage such as the computer viruses, computer hacking and denial of service attacks have become more common, more ambitious and increasingly sophisticated in the networked environment. Increasingly across information systems the interconnection between the public and the private networks and the sharing of the information assets/ resources will increase the difficulty of ensuring security for information and the information systems.

Apart from the technical and administrative measures, which need to be put in place by the organization itself to ensure information security; legal responses to tackle and prevent

such information security breaches are essential to ensure that information systems are protected legally and there are effective recourses available against offenders and hackers. Governments across the world are realising the importance of having effective legal responses to hacking and misuse of information systems and have enacted various laws in this regard. This paper explores some such legal responses by relevant Governments. At the outset it is clarified that this paper will not deal with data protection laws, which is different from information security laws, which will be the subject matter of this paper.

7.2 OBJECTIVES

After studying this unit, you should be able to:

- familiarize yourself with the threat to information systems in different jurisdictions;
- know the different legislatures enacted to counter such threats in India; and
- know the different legislatures enacted to counter such threats in US.

7.3 INDIA

7.3.1 The Information Technology Act, 2000

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. The Act is a first step towards making e-commerce and e-transactions in India safer and a viable alternative to paper based transactions. The Act provides various mechanisms which encourage and recognise information security measures chief amongst them being digital signatures.

Digital Signatures

The Act has adopted the Public Key Infrastructure (PKI) for securing electronic transactions. As per Section 2(1) (p) of the Act, a digital signature means an authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the other provisions of the Act. Thus a subscriber can authenticate an electronic record by affixing his digital signature. A private key is used to create a digital signature whereas a public key is used to verify the digital signature and electronic record. They both are unique for each subscriber and together form a functioning key pair.

Section 5 provides that when any information or other matter needs to be authenticated by the signature of a person, the same can be authenticated by means of the digital signature affixed in a manner prescribed by the Central Government. Under Section 10, the Central Government has powers to make rules prescribing the type of digital signature, the manner in which it shall be affixed, the procedure to identify the person affixing the signature, the maintenance of integrity, security and confidentiality of electronic records or payments and rules regarding any other appropriate matters.

Furthermore, these digital signatures are to be authenticated by Certifying Authorities (CAs) appointed under the Act. These authorities would inter alia have the license to issue Digital Signature Certificates (DSCs). The applicant must have a private key that can create a digital signature. This private key and the public key listed on the DSC must form the functioning key pair.

Once the subscriber has accepted the DSC, he shall generate the key pair by applying the security procedure. Every subscriber is under an obligation to exercise reasonable care and caution to retain control of the private key corresponding to the public key listed in his DSC. The subscriber must take all precautions not to disclose the private key to any third party. If however, the private key is compromised, he must communicate the same to the Certifying Authority (CA) without any delay.

Issuance, Suspension and Revocation of Digital Signature Certificates

As per Section 35, any interested person shall make an application to the CA for a DSC. The application shall be accompanied by filing fees not exceeding Rs. 25,000 and a certification practice statement, or in the absence of such statement any other statement containing such particulars as may be prescribed by the regulations. After scrutinizing the application, the CA may either grant the DSC or reject the application furnishing reasons in writing for the same.

While issuing the DSC, the CA must *inter alia*, ensure that the applicant holds a private key which is capable of creating a digital signature and corresponds to the public key to be listed on the DSC. Both of them together should form a functioning key pair. The CA also has the power to suspend the DSC in public interest on the request of the subscriber listed in the DSC or any person authorized on behalf of the subscriber. However, the subscriber must be given an opportunity to be heard if the DSC is to be suspended for a period exceeding fifteen days. The CA shall communicate the suspension to the subscriber.

There are two cases in which the DSC can be revoked. Firstly, as per Section 38 (1), it may be revoked either on the request or death of the subscriber or when the subscriber is a firm or company, on the dissolution of the firm or winding up of the company. Secondly, according to Section 38(2), the CA may *suo moto* revoke it if some material fact in the DSC is false or has been concealed by the subscriber or the requirements for issue of the DSC are not fulfilled or the subscriber has been declared insolvent or dead et al. A notice of suspension or revocation of the DSC must be published by the CA in a repository specified in the DSC.

Computer Crimes

The Act deals with some more computer crimes and provides for penalties for these offences. Chapters IX and XI of the Act deal with civil liabilities for offences and criminal offences respectively. Civil liabilities and awarding of compensation or damages for certain types of computer frauds has been provided for in the Act.

Section 65 punishes tampering with computer source documents with imprisonment up to three years, or with fine, which may extend up to two lakh rupees, or with both. Computer source code; is defined as the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Section 66 punishes hacking with computer system, with imprisonment up to three years, or with fine which may extend upto two lakh rupees, or with both.

Section 72 Penalty for breach of confidentiality and privacy, imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Acting as an intermediary between various people accessing the net, Internet Service Providers run the risk of being held liable for information that is transmitted over his service network. Chapter XII of the Act excludes the Network Service Provider from any civil or criminal liability under the Act, Rules or Regulations framed thereunder, for

any third party information or data made available by him, if, he proves that the offence was committed without his knowledge, or that he had exercised all due diligence to prevent the commissioning of such offence.

Proposed Amendments to the IT Act 2000

In the wake of growing importance of the need to protect information systems the Government of India has proposed certain amendments in the IT Act 2000 aimed at achieving this goal. Section 43 of the IT Act is proposed to be amended to say, if any body corporate, that owns or handles sensitive personal data or information in a computer resource that it owns or operates, is found to have been negligent in implementing and maintaining reasonable security practices and procedures, it shall be liable to pay damages by way of compensation not exceeding Rs. 1 crore to the person so affected. Reasonable security practices and procedures have been defined as such security practices and procedures as appropriate to the nature of the information to protect that information from unauthorized access, damage, use, modification, disclosure or impairment, as may be prescribed by the Central Government in consultation with the self-regulatory bodies of the industry, if any.

Section 66 of the IT Act while making unauthorized access of a computer system an offence, also makes unauthorized downloading/ extraction of data also an offence.

Under the proposed amendments to Section 72 of the IT Act, if any intermediary who by virtue of any subscriber availing his services has secured access to any material or other information relating to such subscriber, discloses such information or material to any other person, without the consent of such subscriber and with intent to cause injury to him, such intermediary shall be liable to pay damages by way of compensation not exceeding Rs. 25 lakhs to the subscriber so affected. Further the amendments to Section 72 also propose to make video voyeurism an offence under the Act.

7.3.2 RBI Guidelines on Information Security Applicable to Banks in India

The Reserve Bank of India, which is the apex authority governing functioning of the banking sector in India, has given detailed guidelines, which are applicable to all Banks operating in India regarding information security in the Banks. The Guidelines are detailed and address almost all issues relating to information security have been addressed. The guidelines are in time to ensure safety in the banking sector in India.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Is there any protection for Digital Signatures in India? What method has the Act adopted?

.....

.....

.....

.....

.....

.....

7.4 UNITED STATES OF AMERICA: THE CFAA, DMCA AND CASE LAWS

7.4.1 Computer Fraud and Abuse Act (CFAA)

The starting point for a discussion of the current United States law of information security is the Computer Fraud and Abuse Act (18 U.S.C. 1030), (the "CFAA"). The CFAA imposes both civil and criminal liability for a wide variety of acts that compromise the security of public and private sector computer systems.[1]

The core provisions of the CFAA apply to "protected computer[s]," a term that the act defines in sweeping terms. Under the CFAA, the term "protected computer" means "a computer –

1. "exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government;" or
2. "which is used in interstate or foreign commerce or communication" [18 U.S.C. 1030 (e)(2)].

The CFAA imposes liability on anyone who:

1. Intentionally accesses a protected computer without authorization or in excess of authority, and by doing so, steals anything of value, other than the use of the computer itself, where that computer use is worth less than $5,000 in any one year period [18 U.S.C. 1030 (a)(4)];
2. Knowingly transmits a program, code or instruction, and as a result, intentionally causes damage, without authorization, to a protected computer [18 U.S.C. 1030 (a)(5)(A)];
3. Intentionally accesses a protected computer without authorization, and as a result, causes damage, recklessly or otherwise [18 U.S.C. 1030 (a)(5)(B)];
4. Knowingly traffics illegally in passwords or other access credentials that allow unauthorized access to a computer, if that traffic effects interstate or foreign commerce or the computer is used by or for the United States government [18 U.S.C. 1030 (a)(6)]; and
5. Threatening to damage a protected computer with intent to extort anything of value [5]; or
6. Attempts to do any of the above[1] [18 U.S.C. 1030(b)].

Private parties 'who suffer loss or damage' as the result of a CFAA violation have the right to sue [18 U.S.C. 1030(g)].

7.4.2 The Digital Millennium Copyright Act (DMCA)

The Digital Millennium Copyright Act (17 U.S.C. 1201- 05), (the "DMCA"), provides that "no person shall circumvent a technological measure that effectively controls access to a work protected" under the copyright law of the USA and goes on to prohibit the "manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that —(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively

controls access to a copyrighted work; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a copyrighted work; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a copyrighted work." The DMCA defines the term "circumvent a technological measure" to mean to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner 17 [U.S.C. 1201 (a)]. This provision of the DMCA assists licensors of digitized copyrighted works in restricting access to those who obtain access to it lawfully and are therefore entitled to decrypt the work.

The DMCA contains analogous provisions prohibiting technology that circumvents "the protection afforded by a technological measure that effectively protects a right of a copyright owner." The DMCA also: (a) defines the term "circumvent protection afforded by a technological measure'' [to] mean avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and (b) states that a technological measure "effectively protects a right of a copyright owner under this title'' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner [17 U.S.C. 1201 (b)]. This provision gives copyright owners legal recourse against anyone who removes technology that limits the use of copyrighted works to the uses authorized by the owner.

Like the CFAA, the DMCA imposes both criminal and civil liability. With regard to civil remedies, the DMCA provides for the recovery of actual damages, the violator's profits, and statutory damages ranging up to $2,500 per act of circumvention, or per device, product, component, offer, or performance of service. Damages may be trebled (tripled) where the injured party proves that the current violation occurred within three (3) years after the entry of judgment against the defendant for a previous violation. Injunctive relief and the recovery of attorney's fees are also available [17 U.S.C. 1203].

It is to be noted that the DMCA looks at circumvention technology designed to circumvent copyrighted works..

7.4.3 eBay Case in the US

Though the law in India is not very well developed in cases of information security there are cases in the US which help interpret the broad parameters of the issues involved and provide us with an understanding of the jurisprudence involved:

In eBay Inc. V. Bidder's Edge, Inc. [100 F. Supp. 2d 1058 (ND Cal., May 24, 2000)], eBay, the well known Internet auction service, was confronted by routine, multiple, recursive searches of its database conducted by Bidder's Edge, a now defunct aggregator of auction sites, using software robots that exceeded eBay's limitations on robotic access. Negotiations between the parties aimed at providing Bidder's Edge with additional authorized robotic access to eBay's database were unsuccessful, and Bidder's Edge continued to conduct searches without eBay's authorization, depriving eBay of control of its own system. Ebay sued, seeking an injunction to stop Bidder's Edge from conducting such searches, on a trespass to chattels theory. In ruling for eBay, the court wrote:

"Although there is some dispute as to the percentage of queries on eBay's site for which BE [Bidder's Edge] is responsible, BE admits that it sends some 80,000 to 100,000 requests to plaintiff's computer systems per day. Although eBay does not

claim that this consumption has led to any physical damage to eBay's computer system, nor does eBay provide any evidence to support the claim that it may have lost revenues or customers based on this use, eBay's claim is that BE's use is appropriating eBay's personal property by using valuable bandwidth and capacity, and necessarily compromising eBay's ability to use that capacity for its own purposes. ...The law recognises no such right to use another's personal property. ...If preliminary injunctive relief were denied, and other aggregators began to crawl the eBay site, there appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value. California law does not require eBay to wait for such a disaster before applying to this court for relief." (100 F. Supp. 2d 1058 (ND Cal., May 24, 2000).

7.4.4 Liability in Torts

Further case laws in the US have held that if a company or an organization is negligent in not having adequate technological safeguards which protects information from being hacked, misused or from being lost, then the company or the organization may be held liable for negligence. For example, if Internet Explorer has a security flaw and Microsoft has released a patch for the flaw, which is readily available, and the company fails to install the patch and is hacked or the systems in the company crash due to such vulnerability, then the company is liable for any damages. Under tort law, even though the hacker would be liable in a trespass against the company, the company would be liable, under negligence, for any injuries the hacker caused a third party. For example, if the hacker was able to delete a customer's order from a supplier's computer file, the customer could hold the supplier liable for any damages he sustained by not receiving its order. The negligence theory is based on the fact that the supplier should have installed the necessary equipment (hardware and software) and shall took reasonable actions to prevent the hackers from invading his computer system. Also, because the supplier did not have the necessary protection on its computer system, it should have known that such an act was likely to occur, and, therefore, guarded against it.[2]

In such cases the issues that would crop up during any discussion of liability would essentially be:

1. Did the organization have a duty to protect information, which has been misused, lost or hacked?
2. What measures did the organization take to protect the information stored on its computer systems and information networks?
3. Apply the 'reasonable person' test and see if a reasonable security expert would have taken any other precautions to protect the information and whether you have failed to do that?
4. Was the technological vulnerability known or capable of being known to you—was it known publicly? Would any 'reasonable person' have known about the vulnerability?
5. Was the vulnerability fixable and if so how long had a fix existed? Would a 'reasonable person' have installed the fix prior to the time the hack had occurred?
6. Was that type information stored in a location that any 'reasonable person' would have thought to be acceptable?

Essentially the defence available against an action of negligence as specified above would be to prove that the company has taken all reasonable steps ensure that

information security has been established and any "reasonable person" would do no more in this respect than what the company has done. The following are factors, which may be considered while determining whether the company has done everything reasonably possible to ensure information security. Therefore a company should consider the following steps[3]:

1. Establish a budget and staff with time that is dedicated to system security;
2. If you do not already have one in place create a written security policy;
3. As part of your security policy, develop and implement a procedure that tracks security risks and as they are identified, evaluates their potential risk to your business, identifies the appropriate fix, and schedules a date for implementation of that fix. Include follow-ups to ensure that the fix has been completed;
4. Check with your systems/OS vendor and find and implement all suggested lock down procedures for your OS and Hardware;
5. Install a good firewall. Roughly eighty per cent of all attacks happen from within the firewall but you still need to protect against the other twenty per cent;
6. Employ some form of Intrusion Detection and monitor it regularly;
7. Keep yourself and your staff educated on the latest in security and vulnerabilities;
8. Review security resources such as Bugtraq, SANS, Securityfocus, virus reports and other security publications, books and web sites as well as vendors websites on a regular basis;
9. Perform regular security audits on your systems and networks. These can be done internally but should also be done on a regular basis by an independent auditing firm that specializes in security auditing. Read the results of your audits carefully and act on any holes found in your security, procedures and policy;
10. Make sure your company has a security awareness program for all employees. Whether through social engineering or leaving sensitive information displayed on an unattended computer screen, a good security policy does no good if your employees are unwittingly releasing information to a hacker;
11. Properly destroy all unusable media and printouts. Use a professional information destruction company or at a minimum run all unusable tape and printouts through a shredder. When a hard disk drive is upgraded or replaced, the old drive must be sanitized or destroyed;
12. If you organization which is providing information technology services to companies outside India, educate your self on applicable laws in jurisdictions where your contracts will be governed and make sure you lock down your systems and networks according to such applicable laws;
13. Make sure you understand and abide by any other laws that may cover the types of information and data being handled on your systems and networks;
14. Use Data Encryption in the transmission and storage of sensitive data; and
15. Do everything you can to maximize security but get insurance. Review your insurance policies and if your insurance does not cover your business for situations regarding hacking losses and/or online liabilities, get covered.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 4 Min.*

What is the difference between the CFAA and the DMCA?

.....

.....

.....

.....

.....

.....

.....

.....

Let us now summarize the points covered in this unit.

7.5 SUMMARY

- Information security incidents have been on a rise.
- Organizations and individuals have had to suffer a lot of damage.
- India has inadequate laws to deal with such information security issues.
- The Information technology Act, 2000 provides various mechanisms which encourage and recognise information security measures.
- The Act has adopted the Public Key Infrastructure (PKI) for securing electronic transactions.
- The Act deals with some more computer crimes and provides for penalties for these offences. Chapters IX and XI of the Act deal with civil liabilities for offences and criminal offences respectively.
- India needs to develop jurisprudence on these laws.
- US and UK laws have evolved but are still facing myriad technological challenges and are struggling to keep pace with the changes.

7.6 TERMINAL QUESTIONS

1. In the age of information why is it important to protect one's information systems against various cyber security threats and vulnerabilities?
2. Explain in brief the legal treatment of Information Security in the Information Technology Act, 2000.
3. Explain in the brief how the United States of America has addressed the issue of information security and technological vulnerabilities in its legislations.
4. Critically analyse the case the eBay Inc. V Bides edges Inc. in the Context of Information Securities and the Legal Principal Programmed.

5. Analyse and explain the concept of negligence in tort and its relationship to information security and how liability may be imposed on an individual or an organization through the concept of negligence.
6. What is the defence available to a charge of negligence in the context of information security and what processes/policies should an individual/company have in place to substantiate such defence?

7.7 ANSWERS AND HINTS

Self Assessment Questions

1. Yes. Adoption of Public Key Infrastructure and creation of Certifying Authorities.
2. One is for the protection of computers while the other protects copyrights.

Terminal Questions

1. Refer to section 7.1 of the unit.
2. Refer to section 7.3 of the unit.
3. Refer to section 7.4 of the unit.
4. Refer to section 7.4 of the unit.
5. Refer to section 7.4 of the unit.
6. Refer to section 7.4 of the unit.

7.8 REFERENCES AND SUGGESTED READINGS

1. Steven Robinson. "US Information Security Law". Security Focus.com. 10Mar.2007<http:// www.securityfocus.com>.

2. Gary Holtz. "System Security and Your responsibilities. Minimizing your Liability". Sans.org. 10Mar.2007<http://www.sans.org/rr/whitepapers/legal/46.php>.

3. Ibid.