

# Security, privacy and ethics

Technology, Information Technology



ID # Security, Privacy and Ethics Introduction At the present, the use of modern technologies such as information systems, computer networks and databases has become essential for the business organizations. Without a doubt, they offer a wide variety of advantages and opportunities for all kinds of businesses. On the other hand, they also cause many issues regarding security, privacy and ethical attacks. In this scenario there is a vital need for the adoption of enhanced security and privacy solutions. In addition, the application of such security based solutions demands effective security management knowledge and expertise. With the implementation of effective security mechanism we can gain a great deal of confidence and peace of mind while using these systems at home or marketplace (Shelly, Cashman and Vermaat; Turban, Leidner and McLean). This paper presents some of the security, privacy and ethical aspects regarding information technology and computer systems.

#### Security, Privacy and Ethical Issues

There are many issues and threats which are hindering the successful operation and working on information and computer system arrangements. In this scenario, one of the initial risks is security issues from less effectively recruited staff personnel. For instance, any staff member with some illegal aims and objectives can set a virus in the database or hack the overall corporate information. Additionally, this is one of the major ethical dilemmas in information and computer systems (UN; Farshchi, Gharib and Ziyae). In addition, differences in operating systems, versions and patches can also create various problems and issues regarding defense and protection of information and computer systems. In the absence of such protection

strategy the overall information and data can be hacked or deleted. In worst case the business information can be accessed by corporate competitors. Additionally, absence of antivirus software for information and computer systems can also cause a huge problem for personal or business data and information. In case of such situation any virus can simply attack and destroy or stop the overall working of systems. In addition, one of the main issues is about the absence of internal firewalls. In this scenario, any user of systems and web services are open to virus attacks, malware, or Trojan attacks. In such situation overall information and computer systems can be hacked or influenced in case of effective handling and management of operations (UN; Farshchi, Gharib and Ziyadee).

#### How Security, Privacy and Ethical Issues Happen?

This section discusses how some of the major and critical security, privacy and ethical issues happen. These issues can be about single network, corporate, business, shop, individual or any kind of person: (UN; Farshchi, Gharib and Ziyadee; Mookhey)

Lack of suitable security policies

No enhanced cryptographic modules

No Backups

No recording logs for users from external interaction

Have no suitable intrusion detection system

No facility of backup snapshots

Have no Secure File Transfer Protocol (SFTP)

Have no Secure Socket Layers (SSL)

No suitable and updated anti-virus and anti-spyware software

There is no documented policy

There is no content filtering

There is no documentation for any of the setup

There is no firewall in existence

### Security, Privacy and Ethical Issues Mitigation

This section presents the mitigation and management of critical security, privacy and ethical Issues. This section outlines some of the major methods and techniques for implementing countermeasures and prevention techniques for dealing with viruses, worms, logic bombs, Trojan horses and other related forms of security, privacy and ethical issues. In this section I have suggested some of the important methods and techniques those will be used for the enhanced and effective management of security, privacy and ethical issues: (Magalhaes; Danchev)

#### Firewalls

Information technology and computer systems can be protected through firewall system that is an essential element of network which is used by the people to access the Internet.

#### Service packs

For information and computer systems service packs are an essential technology. It basically encompasses new definitions of virus and attacks those can be handled through such technology setup.

#### Antivirus

This is also one of most important security management solutions used by approximately all individuals and organizations for the overall management of security and privacy.

## Strong password practices

In order to protect a system against the outsider attacks we need to build strong passwords. In this scenario we need to choose less frequently used names and numbers so that an outsider cannot gain access to our system.

## Other Solutions

Digital Signatures and Certificates

Secure Socket Layers

PCI, SET, Firewalls and Kerberos

Advanced Data Encryption

Instant Suspicious Activity Notifications

Payment Processing Technology

## Conclusion

At the present, the use of information technology has become for all the businesses and industries. Despite a number of advantages of information technology there are certain issues also involved with the implementation of information technology. In this scenario, information security, privacy and ethics are some of the most important issues that need to be addressed in order to make best use information technology. In addition, there are many solutions and techniques which can be adopted to deal with these issues.

## Works Cited

Danchev, Dancho. Building and Implementing a Successful Information Security Policy. 2003. 03 December 2012 .

Farshchi, Seyyed Mohammad Reza, Fariba Gharib and Reza Ziyaaee. " Study

of Security Issues on Traditional and New Generation of E-commerce Model."

2011 International Conference on Software and Computer Applications  
IPCSIT vol. 9 (2011). Singapore: IACSIT Press, 2011. 113-117.

Magalhaes, Ricky M. Hardening Windows NT/2000/XP Information Systems.  
23 July 2004. 19 November 2012 .

Mookhey, K. K. Common Security Vulnerabilities in e-commerce Systems. 02  
November 2010. 27 November 2012 .

Shelly, Cashman and Vermaat. Discovering Computers 2005. Boston:  
Thomson Course Technology, 2005.

Turban, Efraim, et al. Information Technology for Management: Transforming  
Organizations in the Digital Economy. New York: Wiley, 2005.

UN. Youth and Information and Communication Technologies (ICT). 2003. 25  
November 2012 .