International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Issues in IT & Information Security System Development

Shakila Shams[1], M. Abdus Sobhan[2], Farruk Ahmed, Ph.D.[3], Ali Shihab Sabbir, PhD[4]

[1]The Independent University Bangladesh, Computer Network &Communication (M.Sc.Eng.), Computer Science & Engineering (CSE)
Plot 16, Block B, Aftabuddin Ahmed Road, Bashundhara R/A, Dhaka-1229, Bangladesh
shamsshakila2[at]gmail.com

[2]Vice Chancellor of Prime University, 114, 116 Mazar Rd, Dhaka 1216, Bangladesh
asobhan[at]secs.iub.edu.bd
masobhan.primeuniversity[at]gmail.com

[3]Department of Computer Science & Engineering, Ph.D. in Electrical and Electronic Engineering, 1979,
University of Salford, Manchester, England
farruk[at]iub.edu.bd

[4]Department of Computer Science & Engineering, The Independent University Bangladesh
Plot 16, Block B, Aftabuddin Ahmed Road, Bashundhara R/A, Dhaka-1229
asabbir[at]iub.edu.bd

Abstract: ***Rapidly acceleration the evolution of technologies, the ubiquity of computers as well as heightening connectivity through the Internet has provided numerous benefits for people, society, professional life and businesses sector etc through issues in IT & Information Technology for development. In fact, every aspect of life has somehow changed because of these advances and improvement of rapid acceleration of IT & Information Technology System is observed considering improvement of informational technology system. Many opportunities for creating jobs, technologies and businesses have surfaced because of technological improvement. However, it cannot be denied that these developments come along with challenges adventures improvement, one of which pertains to information security system. Information security system level area refers to the protection of information as well as its accompanying "critical condition", including the systems and hardware that use, store, and transmit that information." This is highlighted in these terms.***

Keywords: Internet Security Law & Legal Issues, Ethical Issues, Professional Issues, Security Issues in Information Technology, Data Privacy & Security System

1. Introduction

As a future information security system sector considering on these legal approachments, ethical, professional division area, you must understand the scope of an organization's legal and ethical issues, professional responsibilities and processment method level. The information security system legal, logical, ethical approchment system and professional plays an important role in an organization's approach mental improvement success to managing liability for privacy and security risks system in every aspect in technological improvement which is discuss in these level. In the modern litigious societies of the world and globally, sometimes laws are enforced in civil courts or circumstances, where large damages can be awarded to plaintiffs who bring suits against organizations or job sector. Sometimes these damages are punitive—assessed as a deterrent. To minimize liability and reduce risks or obstacles from electronic and physical threats or panicness, and to reduce all losses from legal action, information security practitioners system must thoroughly understand the current legal environment sector, stay current with laws and regulations, and watch for new and emerging issues and processment system level. By educating the management system protocol area level sector and employees of an organizational processment on their legal ethics and ethical obligations and the proper use of information technology and information security system area, security professionals can help keep an organization focused on its primary objectives or purposes and its logical improvement& IT sector. In the first part of this era, you can learn about the legislation and regulations or policies that affect the management of information in an organization or many more sectors. In the second part of this sector, you can learn about the ethical issues or policies related to information security system, and about several professional organizations with established codes of ethics legally. Use this purposes as both a reference sector level to the legal aspects of information security system& technological improvement scenario& technological improvement and as an aide in planning your professional career observing legal ethical concept and idea based improvement.

2. Internet Security Law & Legal Issues

Internet security system is a subset of actions which is aimed at securing information based on computers system and in transit between them. In the modern environment the two subjects are closely linked which is observed. Neither computers nor the networks that connect them are inherently secure system. Computers were subject to attack before the Internet Security System became a public utility system—because illegitimate software hidden on commercial diskettes

could be fashioned to load itself on a computer and play havoc greatly with data in memory or placed on a fixed drive. The Internet, by its very nature related—initially conceived of as an open network to facilitate free exchange of ideas and information—is vulnerable. According to the Internet Soft switch Consortium (ISC), which conducts four surveys each year, in January 2006 there were some 395 million Internet hosts in operation—and billions of computers consulting billions of pages carried by those hosts. Despite best efforts which is observed in every respect, a system of this size and complexity will inevitably have points of entry that can be abused—and software programs frequently have unknown weaknesses that hackers (for fun) or criminals (for gain) discover and turn to their advantage until the flaws are fixed and noticeable.

Computer networks system hold valuable and often protected system, private information, not least data on identities; credit cards; financial data; technical, trade, and government secrets; mailing lists; medical records; and the list could be continued considering every sources. These data are vulnerable on the computer and in transit related system. The Internet, as a connector between computer systems and other internet security system, is also a highway of access to valuable data stores. The vulnerabilities are loss of data system through malicious erasure, the acquisition of proprietary information, the manipulation of the data such as illegal withdrawals and transfers of funds, the capture and criminal related misuse of credit cards and many more system or identities, and any and all unauthorized uses to which information may be put. Internet security system to improve breaches can also potentially have direct physical consequences matters if the wrong people hijack systems that control transportation or power related systems through information technology system to highlight or improvement of IT & Information Technology system. Computers have become so pervasive, and their networking so universal, that Internet security system and security in general are closely linked objectives of society in every respect in our life and every purposes.

3. Ethical Issues

Ethics is integral in any aspect of life behavior because it guides people to do what is considered right. Doing the right thing ensures not only success and opportunity but also the avoidance of harm to different stakeholders. Because of this, there are professional organizations which indicate some ethics that have made it their responsibility to develop and enforce codes of ethics legally so that the professional's ethics in their fields would not have alibis for doing the wrong thing or activities. These professional organizations have the authority to remove any practitioner proven to have behaved unethically issues logically and also illegally so that the integrity of the profession is kept intact and to avoid any kind of losing the public's trust and beliefs considering ethical issues and considerations for improvement of information security system according to IT developments in every aspect of life.

However, even if professional organizations have already been established within the information technology and information security system related sectors, they still have not yet developed a binding code for ethical practices mainly because technology continues to evolve. These associations, including the Information Systems Security area, Association, can only recommend ethical practices but they really do not have the authority to remove unethical members from position. As a result, unethical practices have been rampant especially as technology advancements that may be used to enhance trade and even politics are currently being used in unethical or illegal ways but you have to protect issues in IT & Information security system and also enhance its developments.

Among the most common ethical issues criteria system level areas pertaining information security are (i) infringement on software licenses & certification; (ii) spreading of viruses and hacking& tracking; and (iii) misuse of company equip mental improvement scenario. As of now, there are no clear guidelines, rules & regulations pertaining to these practices other than the legal repercussions of such acts & activities. Those that commit them generally do not feel that they are obliged to follow ethical behaviors prescribed for those who are in this field which is discuss in these terms.

Software infringement is also known as software piracy, tracking system, fragmentation, management, and policy. People from different parts of the world are aware of what software piracy means but not all of them believe that it is unethical which is discussed in these terms. As a result of this, major software companies are losing roughly 35% to 40% of their potential revenue to software pirates around the world. Software piracy involves the illegal copying, tracking detecting, tracking system, distribution and sale of commercial software system. Today, hacking through unsecure websites or sources, expired or hacked domain names, or old Internet protocols are a major organized activity that thrives through the vast network, communication system of criminal and syndicates all over the world in the scenario system.

Indeed, individuals are the lowest defense against external attacks and "the most dangerous to the organization. A higher percentage of culprits for illicit use are not the external hackers& trackers, but the employee who has intimate knowledge and access to organizational systems and who are able to obtain permissions by individuals sectors area - properly or improperly - to access sensitive information and security system level. On the other hand, many employees across the world misuse company resources such as computers& other related high quality technologies& system. An example of this is using company computers for personal reasons like sending personal emails or playing games or other amusement system areas sector. In spite of this common occurrence, most employees do not perceive this as an unethical practice and consequences and their conditions and consequences which is discussed in these terms for development of IT & Information security system level.

4. Professional Issues

Aside from the legal and ethical issues and its influences involved in the enforcement of security system of information, there are also professional issues or activities related to this field. Information security system professionals are very important in addressing the legal issues discussed earlier or in advance, and they need to be trained and well-informed about the legal external environment situation. In doing so, they will be more effective in every sector performing one of its tasks, which is to help in maintaining information security system by contributing to the development and enforcement of company policies and issues. In turn of these policies serve as laws& regulations within the organization and have their own set of provisions, penalties as well as sanctions so that compliance is ascertained which is high lightened in these terms. It is important to note, however, that there is a significant difference between legislation and policies or issues - "ignorance or negligence of a policy is an acceptable defense." In light of these, there are certain elements information security system professionals need to keep in mind when developing and enforcing policies or issues are:

Policies must be distributed or organized and duly understood by employees who are expected to adhere with them systematically;

These must be readily acceptable scenario knowledge available in the event that employees want to review them with careful technologies system considering society or workshop to improve information security system;

They should be easily understood and if necessary, translated into different languages or activities and be in a form that may be reviewed by illiterate or visually impaired workers or employees; and Acknowledged by workers or employees in the form of signed forms.

Meanwhile, deterrence and preventive measures are generally acknowledged as the solution and its consequences to unethical practices impacting information security system. Information security system professionals also face certain issues as to the roles they can place in deterrence. First, these professionals have to be properly educated or literal power and trained with regards to "designing, publishing and disseminating organization policies or issues and relevant laws or policies." They should also learn how to get employees agree to comply with these policies, which is something that could make them as the least well-liked persons or fellowship in the organizations. Many employees, including those in leadership positions, could not fully appreciate the importance of implementing certain protocols or rules with regard to computer use highly in society area. They would think that information security system experts are being unreasonable or causeless and overly paranoid with regards to their systems. This is understandable or reasonable because they do not understand how risks or obstacle could originate or commence from activities that seem to be harmless in nature considering circumstances or situation related works, such as visiting websites or downloading materials from the Internet technology which is sometimes also effect on society. May be it creates conflict between society and professional issues applying information technology& IT applications. In relation to this, IT professionals must take the time to explain to the workforce why certain measures or materials (including launching ethical cyber war attacks) may be necessary and how they would also benefit from following the policies governing computer use or policies.

Another issue or policies confronting professionals is that employees who have the authority and special privilege are the ones who sometimes accidentally damage technological security systems policies. For instance, executives or subordinate may be given full access to all information and without realizing it, one of these executives could introduce virus or antivirus into the system through their electronic devices plugged into their own workstations or organization. There is no intent to harm but it could happen. Thus, information security professionals or job sector have to be effective in their role in planning and control that could prevent such accidents. Just as importantly, professionals have to learn to recognize possible criminal intent OR content and they can do this by having the competence to recognize security system breaches that are caused by accidents or uncomfortable situations, ignorance or negligence and hopeful intention or motivational influences or processment system for issues in IT & Information Technology Security System improvement which is shown in superficial way in below figure: To solve and improvement of social issues (monitoring, junk mail, censorship), professional issues (professional responsibility, codes of conduct), legal issues (software piracy, data protection, legal obligations, computer misuse)

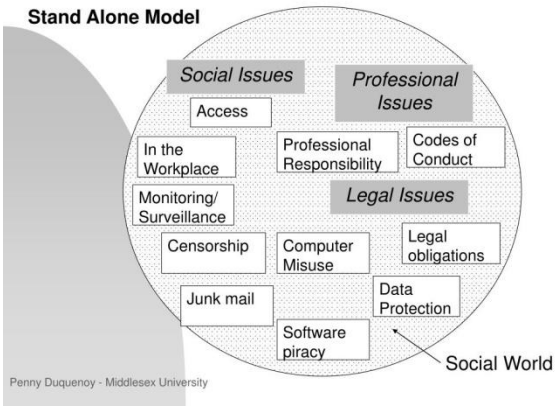

Figure 1: Social & Professional issues in IT

Security Issues in Information Technology:

Now that we have acknowledged the amount of data issues that business collects about people, their activities what are the risks and challenges associated with keeping that information secure or security system in Security Issues in Information Technology? Businesses stand to lose consumer confidence , improvements and respect if they allow unauthorized access to customer data analysis. For this reason, businesses take information security and cyber-security seriously influenced in information technology. Despite the importance of protecting customer data analysis, breaches and hacks seem to be more and more common

criteria. Is this a result of appropriate inadequate security measures on the part of the businesses, professional's or are hackers getting better at accessing so-called "secure networks"? The answer is probably both in information technology. In this It has been estimated that business purpose expend more than 5% of their annual IT budgets protecting themselves against disrupted operations& maintenance and theft due to information theft which is you have protect it honestly and carefully for development of information security system & also issues in IT. A February 2018 reported by McAfee estimates that cyber-crime costs the world over $800 billion or 0.08% of global GDP to protect it carefully we have use higher quality IT & Information Security System Development process. Among the reasons given for the growing cost of cyber-crime are which is described in details in below:

- Quick adoption of new technologies by cyber-criminals which have to solve immediately for improvement of information technology.
- The increased number of new users online (these tend to be from low-income countries with weak cyber-security) have to strengthens to materialize improvement of information technology.
- The increased ease of committing cyber-crime, with the growth of Cyber-crime-as-a-Service which is have to develop.
- An expanding number of cyber-crime "centers" that now include Brazil, India, North Korea, and Vietnam such as tremendaous expanding.
- A growing financial sophistication among top-tier cyber criminals that, among other things, makes monetization easier for technological improvement.
- Considering the McAfee report, "Monetization of stolen data, which has always been a problem for cyber-criminals, seems to have become less difficult task because of improvements in cyber-crime black markets and the use of digital currencies" for security in technological improvement in IT sector.

Cyber-crime can take on many faces from data breaches to malicious program that attack a company's network& communications and disrupt service or corrupt sensitive corporate data analysis. We will examine just a few of the ways that criminals are using technology to wreak havoc on business operations for improvement of technological enhancement.

Section of IT sector you'll learn about some of the ongoing security issues for improvement of businesses face in trying to safeguard their authority (and their customers') electronic communications network and data analysis system scenario.

Information technology has presented businesses with opportunities undreamt of only a couple of decades ago for security in information technology. But it also has introduced some unprecedented challenges for enhancement for security in information technological improvement.

Data Privacy & Security System:
Data privacy is still one of the biggest business technology issues around the world. Blockchain technology can solve this problem. We need more and more businesses to understand that block chains don't just serve digital currencies, policies they also protect people's privacy & security system. We also need Amazon, Facebook, Google, etc higher level technology. to understand that personal data belongs in the hands of the individual or personal security system in every sector in life or to solve international problem solution. Mobile security system is a big issue because we rely so much on mobile internet access technology system now a day. We need to be more aware of how these networks & security system can be compromised & discussed and how to protect them to enhance technological improvement system. Whether it's the Iot devices helping deliver data wirelessly to companies or people or other sources using apps on their smart phones or other technological security system. we need to become more aware of our mobile cyber security, other technological system and how to protect our data safety through issues in IT technological security system for improvement of IT sector.

5. Conclusion

Technological advancements and its motivation, the ubiquity of computers and their consequences heightening connectedness brought about by the Internet has provided many benefits to individuals and companies or organization. How people do things some things or works have radically changed time to time because of these technological advancements. However, it is undeniable that these benefits of technological outputs come with certain risks or uncertainty with unexpected computational technology, such as those involving information security breaches that could be unintentional or intentional in nature or circumstances. Information is supposed to be confidential but through technology and information, it has become easily accessible therefore compromising integrity system security technology. Data based security system in technological system stored in databases will have security in place to prevent unauthorized access or retrieval for these purposes for technological benefit. But there are times when individuals will willfully tap into their system to steal or manipulate information for personal gaining power level sector. Other breaches could happen during transmission of data from one network to another and passing the information using the Internet technology.

It must be noted that into the 21st century, information security system has been confronted with increasing ethical or moral, legal and professional issues. There rules and regulations in place that seek to address ethical, legal and professional issues or their influences. However, some of these rules& regulations system in lacking implementation simply because there are many gray areas involving information security system based processment. Hence, it is of utmost importance that information security system professionals be well-prepared through education and training as they play a key role in addressing these problems. Continuous education and training based technology will ensure that best practices are adopted in the workplace in

these terms. Among the things that information security professionals need to master are the relevant laws as they play or motives critical roles in designing and implementing security polices or issues; and, deterrence of unethical behavior considering that they are expected to have the expertise or skillness to accomplish these motivation.

References

[1] Booms, T. E. Hacking into federal court: Employee "authorization" based on technological security system under the guise of stealing personal information& considerations.
[2] Computer Fraud and Abuse Act. Vanderbilt Journal of Entertainment & Technology Law ethics & system based technology, 13(3), 543-575.
[3] Domain Names and Internet Technology. How to Extract Hostnames, fragmentations, Domains, IP address and Subdomains from Internet LinksOr websites Assigned to Different Web Protocols system security?
[4] Hixson, R., & Hunt-Unruh, D. Demystifying HIPAA. Annals of the American Psychotherapy Assn, 11(3), 10-14.
[5] Moores, T. T., Nill, A., & Rothenberger, M. A. Knowledge of software piracy as an antecedent to reducing pirating behavior& technological related information system. Journal of Computer Information Systems, 50(1), 82-89.
[6] Qing,,Zhengchuan, X., Tamara, , & Hong, Does deterrence work in reducing information security policy& private sector through technological improvement abuse by employees? Communications of the ACM, 54(6), 54-60.
[7] Whitman, M.E. &Mattord, H.J. Principles of information security. Independence: