

Chapter 10: Legal, Security, Social and Ethical Issues in Information Systems

10.1 Impact of Information System

An IS in an organization is like the nervous system in the human body: it is the link that connects all the organization's components (human resource, marketing, accounting and finance, operations (i.e. production and service) etc.) together and provides for better operation and survival in a competitive environment. For this reason, the right amount of information at the right time is a key factor for every organization. Every person in the company needs or generates information, and therefore no person in an organization can be totally detached from its IS.

Impact of IS on managers: IS can change the manner in which many decisions are made, and consequently change managers' jobs. Every organization's management makes decision, prepare, plans, and controls activities by using information which is obtained from two major sources namely: formal and informal sources such as face-to-face conversations e.g. telephone calls, social contacts and so on.

Impact of IS on employees:

- People in all jobs benefits in many ways from IS even they are not computer specialists. Since the IS works on the basic systems such as transaction processing and databases, the labor of the clerical work is transferred to the computerized system, and relieving the human mind for better work.
 - Also it creates an information- based work culture in the organization
- Each day IS helps a million of peoples do their jobs more effectively with:
 - greater efficiency,
 - higher quality product or services,
 - better information retrieval,
 - eliminate paper works,
 - Instant share of information etc.
- **In spite** of its positive impact IS has its own negative impact.
- The major limitation or negative impact of IS includes:
 - displace employees (eliminate jobs),

- violate privacy,
 - Information anxiety i.e. frustration, stress, injuries etc. Organizational performance comprises the actual output or results of an organization as measured against its intended outputs

Manager's measure and control organization performance because it leads to:

- better asset management,
- an increased ability to provide customer value,
- improve measures of organizational knowledge and measure of organizational

performance do have an impact on an organization's status. When the performance of the organization is assessed:

- the past management decisions that shaped investments,
- operations and financing are measured to know whether all resources were used effectively, whether the profitability of the business met or even exceeded expectations, and whether financing choice were made prudently.

In general, ISs helps every business company to maintain and provide good service satisfaction for customers & make it possible for companies to manage all their information, make better decisions, and improve their business processes.

10.2 Computer Ethics, Crime, and Privacy

Information Systems Ethics: is a set of concepts or principles that guides us on proper use of information

Information accuracy

- Deals with authentication and fidelity of information

Information property

Deals with who owns information about individuals and how information can be sold and exchanged

Information accessibility

- Deals with what information a person has the right to obtain about others and how the information can be used
- Issues in information accessibility
- Carnivore: software application designed to be connected to Internet

- Service Providers' computers and eavesdrops on all communications.
- Electronic Communications Privacy Act (ECPA): it offered stronger support for voice mail than it did for e-mail. No other laws at federal or state levels protect e-mail privacy
- Monitoring e-mail

The need for a code of ethical conduct

- Business ethics
- Plagiarism
- Cybersquatting: registering a domain name and then trying to sell the name for big bucks to a person, company. Domain names are a scarce resource – one of the few scarce resources in cyberspace

Computer Crime: the act of using a computer to commit an illegal act

- Authorized and unauthorized computer access
- Examples
 - Stealing time on company computers
 - Breaking into government Web sites
 - Stealing credit card information
- Federal and State Laws
 - Stealing or compromising data
 - Gaining unauthorized computer access
 - Violating data belonging to banks
 - Intercepting communications
 - Threatening to damage computer systems
 - Disseminating viruses
- Hacking and Cracking
 - Hacker – one who gains unauthorized computer access, but without doing damage
 - Cracker – one who breaks into computer systems for the purpose of doing damage
- Types of computer crime
 - **Data diddling:** modifying data
 - **Salami slicing:** skimming small amounts of money
 - **Phreaking:** making free long distance calls

- **Cloning:** cellular phone fraud using scanners
- **Carding:** stealing credit card numbers online
- **Piggybacking:** stealing credit card numbers by spying
- **Social engineering:** tricking employees to gain access
- **Dumpster diving:** finding private info in garbage cans
- **Spoofing:** stealing passwords through a false login page
- Computer viruses and destructive code
 - Virus – a destructive program that disrupts the normal functioning of computer systems
 - Types:
 - Worm: usually does not destroy files; copies itself
 - Trojan horses: Activates without being detected; does not copy itself
 - Logic or time bombs: A type of Trojan horse that stays dormant for a period of time before activating

Computer Security – precautions taken to keep computers and the information they contain safe from unauthorized access

- Recommended Safeguards
 - o Implement a security plan to prevent break-ins, Have a plan if break-ins do occur
 - o Make backups!, Only allow access to key employees
 - o Change passwords frequently, Keep stored information secure
 - o Use antivirus software, Use biometrics for access to computing resources
 - o Hire trustworthy employees
- Encryption – the process of encoding messages before they enter the network or airwaves, then decoding them at the receiving end of the transfer
- Internet Security
 - o Firewall – hardware and software designed to keep unauthorized users out of network systems
- Virus prevention
 - o Install antivirus software, Make backups
 - o Avoid unknown sources of shareware, Delete e-mails from unknown sources
 - o If your computer gets a virus...

- How to maintain your privacy online
 - o Choose Web sites monitored by privacy advocates
 - o Avoid “cookies”, Visit sites anonymously
 - o Use caution when requesting confirming e-mail
- Avoid getting conned in cyberspace
 - o Internet auctions, Internet access, International modem dialing
 - o Web cramming, Multilevel marketing (pyramid schemes)
 - o Travel/vacations, Business opportunities
 - o Investments, Health-care products

10.3 Security concerns and security management strategies in e-business applications

Electronic (e-) business, refers to the use of digital technology and the Internet to carry out key business processes within the company. It includes activities for the company's internal management and for coordination with suppliers and other business partners. This also includes e-commerce and it is a part of e-business that deals with the purchase and sale of goods and services through the internet.

E-Business Security Concerns

- Internet can seem like an entrepreneur's dream come true. The Web offers instant access to millions of consumers around the world and the ability to set up a virtual store, which can limit start-up costs. While the Web does offer a powerful platform for launching new venture, e-businesses are subject to a variety of unique security concerns.

Viruses and Other Malware

- E-businesses count on their Web servers and computers to run smoothly to keep business humming along. Computers that communicate with other devices on the Internet have the potential to download malicious software like computer viruses, worms and other malware that can inhibit a machine's ability to function properly. Malware can potentially result in data loss or the need for maintenance, both of which can cost e-businesses time and money. Malware can also impair customers' ability to use their own computers and access e- business sites. According to Consumer Reports, malware cost consumers about \$2.3 billion in 2010.

Software Bugs

The term software bug sounds similar to a virus or worm, which are themselves types of malicious programs, but it means something different entirely. A software bug is simply a mistake or oversight in a computer program or website coding that makes the site or program behave in an unintended way. A bug could result in something relatively benign, like minor aesthetic errors on a website. On the other hand, a bug could potentially cause major problems like site crashes and allowing users access to data that they are not supposed to see.

Active Malicious Threats

While malware can passively infect computers, outside parties can also actively attack web companies. An e-business usually lets users interact with a website, possibly by registering for an account and submitting various forms to the business's web server.

Experienced computer users may be able to exploit weaknesses in a website to gain access to or "hack" into data that they are not supposed to be able to access. Hackers can potentially steal information like customer names, credit card numbers and passwords, or they may inject malicious code into a website that causes data loss.

For example, Sony's PlayStation Network was the victim of a major hacking operation in 2011 that resulted in the theft of millions of users' personal information.

Malicious users may also pretend to be trusted authorities or friends in an attempt to trick employees or managers into divulging sensitive information. This method of stealing data is called "phishing."

Physical Data Theft

Most of the threats to e-businesses come through the Internet itself, but businesses can also be subject to physical data theft. If a thief steals the physical hardware that a company uses to conduct business, such as hard drives or Web servers, he may be able to recover confidential information. Since there are several ways e-businesses can potentially lose important data, it is important to make backup copies of data on a regular basis and ensure that physical plants are secure.

Wireless and Mobile Security

Many businesses use wireless Internet connections and mobile devices to access the Web. Wireless networks present a security hazard, since outside users can attempt to connect to

a wireless network, allowing them to potentially eavesdrop on communications. Securing a wireless network with a password can make it more difficult for outside users to connect to the network and access sensitive information, but a wireless connection is not as secure as a wired connection, even if it has password protection. Mobile devices can be a security concern both because they use wireless communication and because they are easy to misplace.

Security management strategies in e-business applications

- E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. We wanted to take the time to discuss why E-Commerce security is becoming more necessary than ever before and break down steps companies can take to ensure their applications are safe from a vulnerability or data breach.

The importance of securing web applications

- Today, many web apps are experiencing increased use, from online food ordering apps to athleisure, consumers are using web apps more—and hackers are exploiting them more, too. Thus, it is necessary to take web application security seriously and the security implications to not only keep business safe, but customers' data and credit card information, too. Application security is not just one thing you set and forget. It requires testing, monitoring, and adhering to applicable compliance requirements (Payment Card Industry [PCI] ` , for all those revenue-generating apps taking credit cards). Here are the three best practices you need to cover

1. Securing third-party/open-source code

- If you think about the way an app is created, more often than **not**, it's with borrowed code (otherwise known as third-party or open-source code).
- In fact, up to 96 percent of new apps use borrowed code.
- It's a great way to get an app up and running fast and save a lot of development time and resources, but it can also introduce vulnerabilities (that allows an attacker to cause harm to the stakeholders of an application) into your environment.
- Open-source vulnerabilities and exploits in proprietary products share similarities.

- Both involve poorly written code, leaving “holes” or gaps that attackers can use to carry out malicious activities, such as modifying the code to extract sensitive data or damage the system.
- Recent research found that vulnerabilities in open source libraries are growing rapidly.
- That’s where software composition analysis comes in.
- Tools like tCell and InsightVM look at all third-party packages to see if any borrowed code has vulnerabilities.

2. Earlier dynamic web application testing

- Given how fast many web apps have been created over these past few weeks and months, as well as how much traffic they are receiving, it’s important to test your web apps pre-production to identify security weaknesses earlier in the software development lifecycle and ensure your business and users are protected.
- Having the ability to continuously scan for potential issues, especially on apps that drive revenue or are at the forefront of your customer experience, can help mitigate issues before they become one, and keep your business and customers safe.
- It also helps mitigate a breach that could land you in the not-so-favorable news headlines (and can ruin your brand reputation).
- Dynamic Application Security Testing (DAST) solutions
- Like InsightAppSec and AppSpider are built to dynamically scan and test
- modern applications with fewer false positives and are scalable across your entire application portfolio.
- InsightAppSec, for example, is designed to detect more than 95 attack types and offers Attack Replay,
- a feature that allows you to reproduce an issue after you implement a fix to immediately test the work and close out the ticket.
- Want to make sure that you build application security into your development lifecycles?
- Integrate your DAST tool with a Continuous Integration and Continuous

- Delivery or Continuous Development (CI/CD) platform so as new features are released, they are being tested for both quality assurance and any potential security weaknesses.
- It also provides compliance-specific report templates for an immediate understanding of the compliance risk of your web applications.
- Tools like InisghtAppSec are specifically designed to automatically assess modern web apps and APIs,
- fast-track fixes with rich reporting and integrations, keep compliance and development stakeholders informed, and effortlessly scale as your application portfolio grows.
- APIs (Application Programming Interfaces), which is a software intermediary that allows two applications to talk to each other.
- Each time you use an app like Facebook, send an instant message, or check the weather on your phone, you're using an API.

3.

Application monitoring and protection

- With secure code that's been tested for potential vulnerabilities or issues, the last (but equally important) piece is continually monitoring and protecting your application from future issues.
- It's not enough to scan or test once and consider yourself secure. Today, attackers are continuously looking for holes and adapting their attack strategies, so your application needs a way to keep up.
- As e-commerce applications are being used more than ever before, these are prime targets for attack, and it's your job to ensure your apps are protected in order to keep your business and customers safe, and your company name out of the headlines.
- Monitoring and protecting your applications with Next-Gen Web Application Firewalls (WAFs) and Runtime Application Self-Protection (RASP) tools allow you to know that your application is protected in production.
- Tools like tCell by Rapid7 are specifically designed to provide visibility into your application and protection at runtime.
- There are many ways to get a handle on application security, and securing your web applications should be one of the first.
- To get started, check out InsightAppSec and tCell for production and live code scanning to ensure you're not carrying around unwanted vulnerabilities.

10.4 Ethical issues in Information system

- Ethics in ISs can be defined as "ethics that focuses on the relationship between the creation, organization, dissemination, and use of information, and the ethical standards and moral codes governing human conduct in society".
- These ethical issues include:
 - **Information Rights:** Privacy and Freedom in the Information Rights
 - **Privacy:** Most people have their personal data spread throughout the digital world.
 - Even things thought to be secure, such as email or private accounts, can be accessed by unintended sources.
 - Most employers actively check their employees' computer habits.
 - Privacy has evolving legal implications, but there are also ethical considerations.
 - Do people know how their accounts are monitored? To what extent is such monitoring occurring?

Intellectual Property Rights

- Trade secrets
- Copyright
- Patents

Accountability, liability, and control

- Who is liable (legally responsible) for injuries that result from machines controlled by software?
- Computer-related liability problems

System quality: data quality and system errors

- Software bugs and errors
- Hardware or facility failures caused by natural or other causes
- Poor input data quality

The Spamming Problem

- o What are its causes?
- o What techniques/ solutions do you use to shield yourself from spam?
- o How affective are these techniques/solutions

