# Chapter 3

The security of information technology used in business is of utmost importance. Confidential business data and private customer and employee information must be safeguarded, and systems must be protected against malicious acts of theft or disruption.

## Why Computer Incidents Are So Prevalent

* Increasing Complexity Increases Vulnerability
* Higher Computer User Expectations
* Expanding and Changing Systems Introduce New Risks
* Increased Reliance on Commercial Software with Known Vulnerabilities

**Exploit** is an attack on an information system that takes advantage of a particular system vulnerability. Often this attack is due to poor system design or implementation. Once the vulnerability is discovered, software developers quickly create and issue a “fix,” or patch, to eliminate the problem.

A **zero-day attack** takes place before the security community or software developer knows about the vulnerability or has been able to repair it.

## Types of Exploits

Types of attacks

* **Virus:** a virus is a piece of programming code, usually disguised as something else, that causes a computer to behave in an unexpected and usually undesirable manner. Often a virus is attached to a file, so that when the infected file is opened, the virus executes.
* **Worm:** Unlike a computer virus, which requires users to spread infected files to other users, a worm is a harmful program that resides in the active memory of the computer and duplicates itself.
* **Trojan horse:** A Trojan horse is a program in which malicious code is hidden inside a seemingly harmless program.
* **Botnets:** A botnet is a large group of computers controlled from one or more remote locations by hackers, without the knowledge or consent of their owners. Botnets are frequently used to distribute spam and malicious code.
* **Distributed denial of service:** A distributed denial-of-service attack (DDoS) is one in which a malicious hacker takes over computers on the Internet and causes them to flood a target site with demands for data and other small tasks.
* **Rootkit:** A rootkit is a set of programs that enables its user to gain administrator level access to a computer without the end user’s consent or knowledge. Once installed, the attacker can gain full control of the system.
* **Spam:** E-mail spam is the abuse of e-mail systems to send unsolicited e-mail to large numbers of people.
* **Phishing:** Phishing is the act of using e-mail fraudulently to try to get the recipient to reveal personal data.

## Types of Perpetrators

* **Hackers** test the limitations of information systems out of intellectual curiosity—to see whether they can gain access and how far they can go.
* **Crackers** break into other people’s networks and systems to cause harm—defacing Web pages, crashing Crackers break into other people’s networks and systems to cause harm—defacing Web pages, crashing computers.
* **Malicious Insiders**
* **Industrial spies** use illegal means to obtain trade secrets from competitors of their sponsor.
* **Hacktivism**, a combination of the words hacking and activism, is hacking to achieve a political or social goal.
* A **cyberterrorist** launches computer-based attacks against other computers or networks in an attempt to intimidate or coerce a government in order to advance certain political or social objectives.

## Risk Assessment

A risk assessment is the process of assessing security-related risks to an organization’s computers and networks from both internal and external threats.

Eight-step risk assessment process

* + #1 Identify assets of most concern
  + #2 Identify loss events that could occur
  + #3 Assess likelihood of each potential threat
  + #4 Determine the impact of each threat
  + #5 Determine how each threat could be mitigated
  + #6 Assess feasibility of mitigation options
  + #7 Perform cost-benefit analysis
  + #8 Decide which countermeasures to implement

On the one hand, information about people is gathered, stored, analyzed, and reported because organizations can use it to make better decisions. Some of these decisions, including whether or not to hire a job candidate, approve a loan, or offer a scholarship.

In addition, in this competitive global market it is importance to know consumers’ purchasing habits and financial condition. Companies use this information to target marketing efforts to consumers who are most likely to buy their products and services. Organizations also need basic information about customers to serve them better. It is hard to imagine an organization having productive relationships with its customers without having data about them. Thus, organizations want systems that collect and store key data from every interaction they have with a customer.

A combination of approaches—new laws, technical solutions, and privacy policies—is required to balance the scales. Reasonable limits must be set on government and business access to personal information; new information and communication technologies must be designed to protect rather than diminish privacy; and appropriate corporate policies must be developed to set baseline standards for people’s privacy.

“the right to be left alone—the most comprehensive of rights, and the right most valued by a free people.”

Information privacy is the combination of communications privacy (the ability to communicate with others without those communications being monitored by other persons or organizations) and data privacy (the ability to limit access to one’s personal data by other individuals and organizations in order to exercise a substantial degree of control over that data and its use).

# Privacy Laws, Applications, and Court Rulings

The discussion will be broken into the following topics: financial data, health information, children’s personal data, electronic surveillance, export of personal data, and access to government records.

## Financial Data

Individuals must reveal much of their personal financial data in order to take advantage of the wide range of financial products and services available, including credit cards, checking and savings accounts, loans, payroll direct deposit, and brokerage accounts. To access many of these financial products and services, individuals must use a personal logon name, password, account number, or PIN. Individuals should be concerned about how this personal data is protected by businesses and other organizations and whether or not it is shared with other people or companies.

* Financial Privacy Rule—This rule established mandatory guidelines for the collection and disclosure of personal financial information by financial organizations.
* Safeguards Rule—This rule requires each financial institution to document a data security plan describing its preparation and plans for the ongoing protection of clients’ personal data.
* Pretexting Rule—This rule addresses attempts by people to access personal information without proper authority by such means as impersonating an account holder or phishing.

## Health Information

The use of electronic medical records and the subsequent interlinking and transferring of this electronic information among different organizations has become widespread. Individuals are rightly concerned about the erosion of privacy of data concerning their health.

## Children’s Personal Data

Internet use by children continues to climb; a recent report out of the United Kingdom found that teenagers spend an average of 31 hours per week online. As a concerned society, many of us feel that there is a need to protect children from being exposed to inappropriate material and online predators; becoming the target of harassment; divulging personal data; and becoming involved in gambling or other inappropriate behavior.

## Export of Personal Data

Various organizations have developed guidelines to ensure that the flow of personal data across national boundaries (transborder data flow) does not result in the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data.

## Access to Government Records

The government has a great capacity to store data about each and every one of us and about the proceedings of its various organizations. The Freedom of Information Act enables the public to gain access to certain government records, and the Privacy Act prohibits the government from concealing the existence of any personal data record-keeping systems.

# Identity Theft

Identity theft occurs when someone steals key pieces of personal information to impersonate a person. This information may include such data as name, address, date of birth, Social Security number, passport number, driver’s license number, and mother’s maiden name. Using this information, an identity thief may apply for new credit or financial accounts, rent an apartment, set up utility or phone service, and register for college courses—all in someone else’s name.

Four approaches are frequently used by identity thieves to capture the personal data of their victims: (1) create a data breach to steal hundreds, thousands, or even millions of personal records; (2) purchase personal data from criminals; (3) use phishing to entice users to willingly give up personal data; and (4) install spyware capable of capturing the keystrokes of victims.

## Data Breaches

An alarming number of identity theft incidents involve breaches of large databases to gain personal identity information. The breach may be caused by hackers breaking into the database or, more often than one would suspect, by carelessness or failure to follow proper security procedures.

## Purchase of Personal Data

There is a black market in personal data.

## Phishing

Phishing is an attempt to steal personal identity data by tricking users into entering information on a counterfeit Web site.

## Spyware

Spyware is keystroke-logging software downloaded to users’ computers without the knowledge or consent of the user. It is often marketed as a spouse monitor, child monitor, or surveillance tool. Spyware creates a record of the keystrokes entered on the computer, enabling the capture of account usernames, passwords, credit card numbers, and other sensitive information.

## Identity Theft Monitoring Services

There are numerous identity theft monitoring services, which offer a wide range of coverage.

# Consumer Profiling

Companies openly collect personal information about Internet users when they register at Web sites, complete surveys, fill out forms, or enter contests online. Many companies also obtain information about Web surfers through the use of cookies, text files that a Web site can download to visitors’ hard drives so that it can identify visitors on subsequent visits. Companies also use tracking software to allow their Web sites to analyze browsing habits and deduce personal interests and preferences. The use of cookies and tracking software is controversial because companies can collect information about consumers without their explicit permission. Outside of the Web environment, marketing firms employ similarly controversial means to collect information about people and their buying habits.

## Aggregating Consumer Data

Marketing firms aggregate the information they gather about consumers to build databases that contain a huge amount of consumer data. They want to know as much as they can about consumers—who they are, what they like, how they behave, and what motivates them to buy. The marketing firms provide this data to companies so that they can tailor their products and services to individual consumer preferences. Advertisers use the data to more effectively target and attract customers to their messages.

## Collecting Data from Web Site Visits

Marketers use cookies to recognize return visitors to their sites and to store useful information about them. The goal is to provide customized service for each consumer. When someone visits a Web site, the site asks that person’s computer if it can store a cookie on the hard drive. If the computer agrees, it is assigned a unique identifier, and a cookie with this identification number is placed on its hard drive.

## Personalization Software

In addition to using cookies to track consumer data, online marketers use personalization software to optimize the number, frequency, and mixture of their ad placements, and to evaluate how visitors react to new ads. The goal is to turn first-time visitors to a site into paying customers and to facilitate greater cross-selling activities.

## Consumer Data Privacy

Consumer data privacy has grown into a major marketing issue. Companies that can’t protect or don’t respect customer information often lose business and some become defendants in class action lawsuits stemming from privacy violations.

# Workplace Monitoring

Many organizations have developed a policy on the use of IT in the workplace in order to protect against employee abuses that reduce worker productivity or expose the employer to harassment lawsuits.

# Chapter 6

## What is intellectual property?

**Intellectual property** is a term used to describe works of the mind that are distinct, and owned or created by a single person or group. Intellectual property is protected through copyright, patent, and trade secret laws.

**Copyright** law protects authored works, such as art, books, film, and music; **patent** law protects inventions; and **trade secret law** helps safeguard information that is critical to an organization’s success. Together, copyright, patent, and trade secret legislation forms a complex body of law that addresses the ownership of intellectual property.

## What is copyright?

A **copyright** is the exclusive right to distribute, display, perform, or reproduce an original work in copies or to prepare derivative works based on the work. The author may grant this exclusive right to others.

**Copyright infringement** is a violation of the rights secured by the owner of a copyright. Infringement occurs when someone copies a substantial and material part of another’s copyrighted work without permission.

## Copyright Term

Copyright law guarantees developers the rights to their works for a certain amount of time.

## Eligible Works

Types of work that can be copyrighted

* + Architecture
  + Art
  + Audiovisual works
  + Choreography
  + Drama
  + Graphics
  + Literature
  + Motion pictures
  + Music
  + Pantomimes
  + Pictures
  + Sculptures
  + Sound recordings

To be eligible for a copyright, a work must fall within one of the preceding categories, and it must be original. Copyright law has proven to be extremely flexible in covering new technologies; thus, software, video games, multimedia works, and Web pages can all be protected.

## Patents

A **patent** is a grant of a property right to an inventor. A patent permits its owner to exclude the public from making, using, or selling a protected invention, and it allows for legal action against violators. Unlike a copyright, a patent prevents independent creation as well as copying. Even if someone else invents the same item independently and with no prior knowledge of the patent holder’s invention, the second inventor is excluded from using the patented device without permission of the original patent holder.

**Prior art**—the existing body of knowledge that is available to a person of ordinary skill in the art.

An invention must pass four tests

* + Must be in one of the five statutory classes of items
  + Must be useful
  + Must be novel
  + Must not be obvious to a person having ordinary skill in the same field

Items cannot be patented if they are:

* + Abstract ideas
  + Laws of nature
  + Natural phenomena

**Patent infringement**, or the violation of the rights secured by the owner of a patent, occurs when someone makes unauthorized use of another’s patent. Unlike copyright infringement, there is no specified limit to the monetary penalty if patent infringement is found.

A **software patent** claims as its invention some feature or process embodied in instructions executed by a computer.

A **patent troll** is a firm that acquires patents with no intention of manufacturing anything, instead licensing the patents to others.

A patented process or invention that is surreptitiously included within a standard without being made public until after the standard is broadly adopted is called a **submarine patent**. A devious patent holder might influence a standards organization to make use of its patented item without revealing the existence of the patent. Later, the patent holder might demand royalties from all parties that use the standard. This strategy is known as **patent farming**.

## Trade Secrets

Trade secret protection begins by identifying all the information that must be protected—from undisclosed patent applications to market research and business plans— and developing a comprehensive strategy for keeping the information secure. Trade secret law protects only against the misappropriation of trade secrets. If competitors come up with the same idea on their own, it is not misappropriation; in other words, the law doesn’t prevent someone from using the same idea if it was developed independently.

Trade secret law has a few key advantages over patents and copyrights

* + No time limitations
  + No need to file an application
  + Patents can be ruled invalid by courts
  + No filing or application fees

## Key Intellectual Property Issues

Issues that apply to intellectual property and information technology

* + Plagiarism
  + Reverse engineering
  + Open source code
  + Competitive intelligence
  + Trademark infringement
  + Cybersquatting

# Chapter 10

## The Need for Nontraditional Workers

Facing a likely long-term shortage of trained and experienced workers, employers are increasingly turning to nontraditional sources to find IT workers with skills that meet their needs; these sources include contingent workers, H-1B workers, and outsourced offshore workers.

## Contingent Worker

Contingent work is a job situation in which an individual does not have an explicit or implicit contract for long-term employment.

Contingent workers include:

* + Independent contractors
  + Temporary workers through employment agencies
  + On-call or day laborers
  + On-site workers provided by contract firms

Typically, these workers join a team of full-time employees and other contingent workers for the life of the project and then move on to their next assignment.

In **employee leasing**, a business (called the subscribing firm) transfers all or part of its workforce to another firm (called the leasing firm), which handles all human resource- related activities and costs, such as payroll, training, and the administration of employee benefits.

Sources

* + Temporary agencies
  + Employee leasing
  + Consulting organizations

## Advantages of using contingent workers

* + Business does not pay for benefits
  + Can continually adjust the number of contingent workers to stay consistent with its business needs
  + Does not customarily incur training costs

## Disadvantages of using contingent workers

* + Workers may lack a strong relationship with the firm
    - Low commitment to the company and its projects
    - High turnover rate
  + Workers gain valuable practical experience working within a company’s structure and culture
    - Lost when workers depart at the project’s completion

## When deciding to use contingent workers

When an organization decides to use contingent workers for a project, it should recognize the trade-off it is making between completing a single project quickly and cheaply versus developing people within its own organization. If the project requires unique skills that are probably not necessary for future projects, there may be little reason to invest the additional time and costs required to develop those skills in full-time employees.

If a particular project requires only temporary help, and the workers will not be needed for future projects, the use of contingent workers is a good approach. In such a situation, using contingent workers avoids the need to hire new employees and then fire them when staffing needs decrease.

Organizations should carefully consider whether or not to use contingent workers when those workers are likely to learn corporate processes and strategies that are key to the company’s success.

# Chapter 2

A profession is a calling that requires specialized knowledge and often long and intensive academic preparation.

IT workers are not recognized as professionals because they are not licensed by the state or federal government. This distinction is important, for example, in malpractice lawsuits, as many courts have ruled that IT workers are not liable for malpractice because they do not meet the legal definition of a professional.