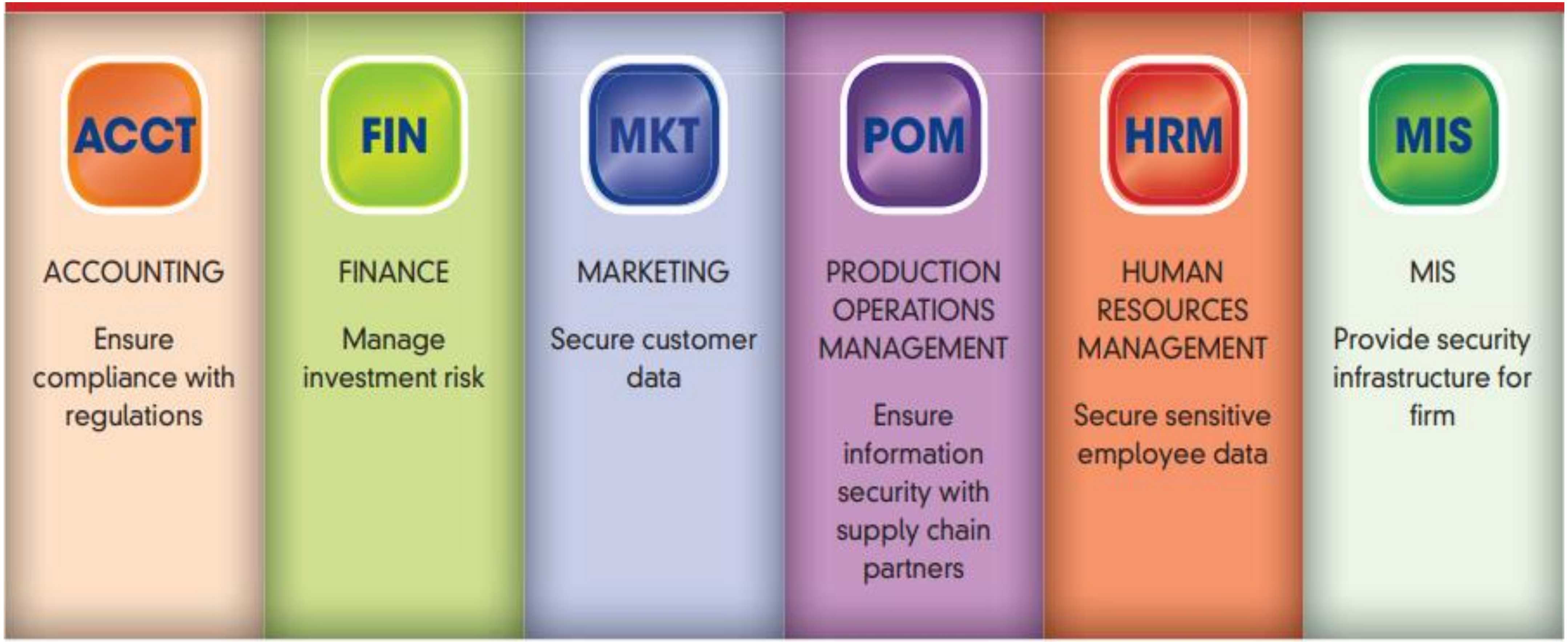
Chapter 3
ETHICAL ISSUES AND PRIVACY

Contents….

- Ethical issues and Privacy
- Information Security.
- Threat to IS, and
- Security Controls



ACCT

ACCOUNTING

Ensure compliance with regulations

FIN

FINANCE

Manage investment risk

MKT

MARKETING

Secure customer data

POM

PRODUCTION OPERATIONS MANAGEMENT

Ensure information security with supply chain partners

HRM

HUMAN RESOURCES MANAGEMENT

Secure sensitive employee data

MIS

MIS

Provide security infrastructure for firm

4.1 Small Businesses in Danger

Picture your graduation day. You have finally completed your undergraduate degree. You initially looked for a job, but you have since decided that you want to start your own business. You pitch your idea to your best friend and ask him/her to join you in a new business venture. Because your degree is in marketing, you would like to start a small promotions business. You and your new business partner develop a solid business strategy, obtain a small business loan from the bank to purchase your computer equipment, and then head over to the courthouse to set up your new Limited Liability Corporation (LLC).

Two years later, things could not have turned out better! Hard work, late nights, and social media exposure have landed your business quite a few clients. The two computers you purchased with your small business loan (one for you and one for your business partner) have turned out to be invaluable. In fact, you now realize more than ever how much you depend on your computers and how lost your business would be without them. You wonder if your antivirus software is up-to-date and if there is anything else you should be doing to protect your critical business data, especially your clients' data. But, you are too busy to research these issues, so you just trust that everything will be OK.

You and your partner have never had such high-quality computers. Fast processors, big monitors, and plenty of memory—all purchased with business intent of course—make these computers superior to the ones you have at home. Naturally you both use your computers for personal work as well. Why not, right?

But then, suddenly, your partner's computer starts to slow down dramatically. Your machine is identical to his, but yours runs much faster. Your partner takes his computer back to Best Buy to have the Geek Squad look it over. The technician determines that **malware** (malicious software) has infected his computer so thoroughly that the hard drive must be replaced. Additionally, the data on his hard drive cannot be recovered, and he has not backed up any of his files—not even the business data.

Now, you have problems. Lost data can result in lost (certainly irritated) customers. In addition, you will have to spend time and money recreating that data.

How could your partner's unprotected Web surfing have resulted in so much lost data? The fact is that even though you both consider yourselves somewhat tech savvy, neither of you ever took steps to protect your computers. You just assumed that a malware infection would never happen to you.

Now, what would you say if you knew that you are not alone? A recent report by GFI Software revealed that more than 40 percent of small- to medium-sized businesses (SMBs) reported a security breach that resulted from an employee visiting a Web site that hosted malware. Amazingly, even though 40 percent of SMBs have experienced this problem, 55 percent reported that preventing this problem from re-occurring was not a priority! Furthermore, 70 percent of the respondents do NOT have any policy about Web use at work, and they claim that Web use is not a problem!

As you can see from this case, installing and maintaining security on computers and information systems is vital to avoid losing business relationships as well as significant amounts of time and money. Fortunately, there are many third-party companies that provide security solutions—see, for example, GFI Software at www.gfi.com. Ultimately, however, you are responsible for seeking out their services and implementing security controls on your own systems and customer data. If you do not prioritize security measures, then you expose your computer and your files to potentially irrevocable damage from thousands of malware systems and viruses.

Sources: Compiled from "GFI Software Survey: 40% of SMBs Have Suffered a Security Breach Due to Unsafe Web Surfing," *Enhanced Online News*, October 12, 2011; "Small Businesses Hacked But Still Not Taking Precautions: Survey Says," *The Huffington Post*, November 7, 2011; www.gfi.com, accessed March 8, 2012.

Questions

1. What security controls should you and your business partner have adopted *at a minimum*?
2. How important are backup plans and file backup procedures to small businesses?
3. Why is it important to protect customer information in businesses of any size?

Antivirus

Software that is designed to detect, stop and remove viruses and other kinds of malicious software.

Botnet

A network of infected devices, connected to the Internet, used to commit co-ordinated cyber attacks without their owners' knowledge.

Bring your own device (BYOD)

An organisation's strategy or policy that allows employees to use their own personal devices for work purposes.

Cloud

Where shared compute and storage resources are accessed as a service (usually online), instead of hosted locally on physical services.

Cyber attack

Malicious attempts to damage, disrupt or gain unauthorised access to computer systems, networks or devices, via cyber means.

Cyber security

The protection of devices, services and networks - and the information on them - from theft or damage.

Denial of Service (DoS)

When legitimate users are denied access to computer services (or resources), usually by overloading the service with requests.

Digital footprint

A 'footprint' of digital information that a user's online activity leaves behind.

Encryption

A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it.

End user device

Collective term to describe modern smartphones, laptops and tablets that connect to an organisation's network.

Firewall

Hardware or software which uses a defined rule set to constrain network traffic to prevent unauthorised access to (or from) a network.

Internet of Things (IoT)

Refers to the ability of everyday objects (rather than computers and devices) to connect to the Internet. Examples include kettles, fridges and televisions.

Macro

A small program that can automate tasks in applications (such as Microsoft Office) which attackers can use to gain access to (or harm) a system.

Patching

Applying updates to firmware or software to improve security and/or enhance functionality.

Phishing

Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.

Ransomware

Malicious software that makes data or systems unusable until the victim makes a payment.

Software as a Service (SaaS)

Describes a business model where consumers access centrally-hosted software applications over the Internet.

Social engineering

Manipulating people into carrying out specific actions, or divulging information, that's of use to an attacker.

Spear-phishing

A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.

Trojan

A type of malware or virus disguised as legitimate software, that is used to hack into the victim's computer.

Two-factor authentication (2FA)

The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

Water-holing (watering hole attack)

Setting up a fake website (or compromising a real one) in order to exploit visiting users.

Whaling

Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.

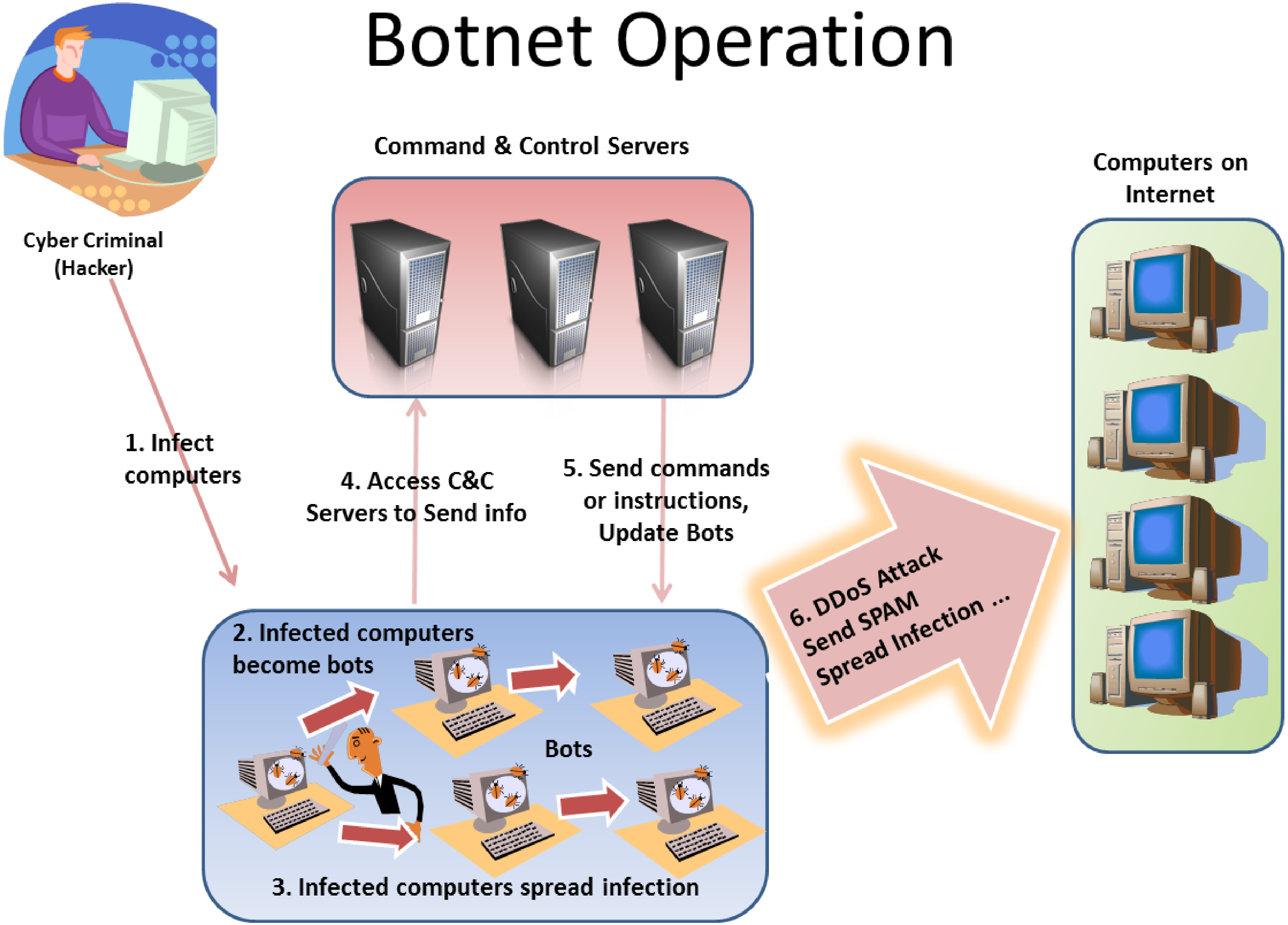
Whitelisting

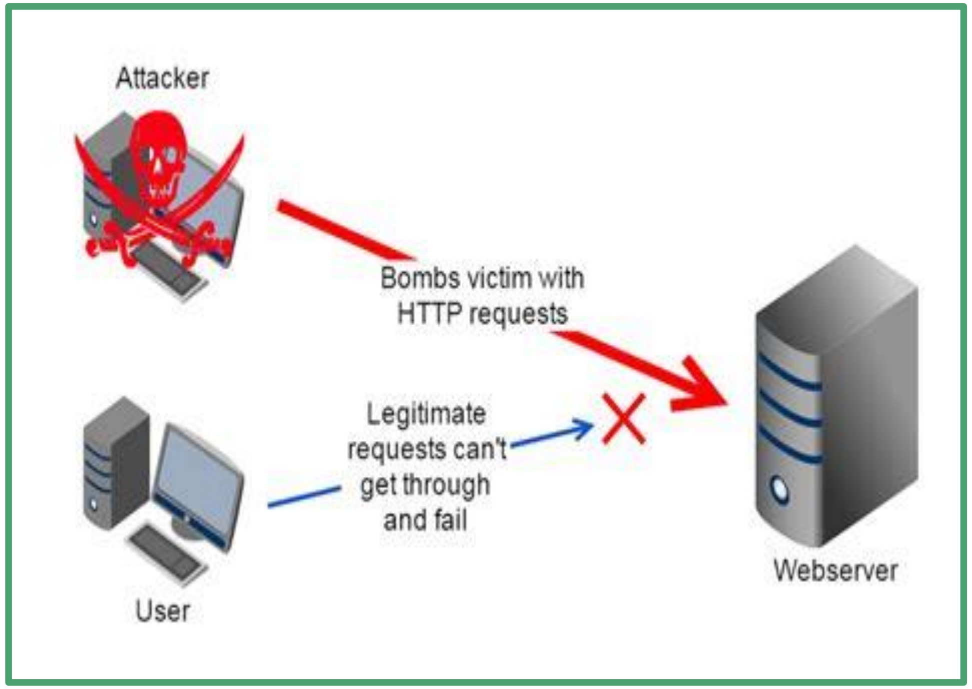
Authorising approved applications for use within organisations in order to protect systems from potentially harmful applications.

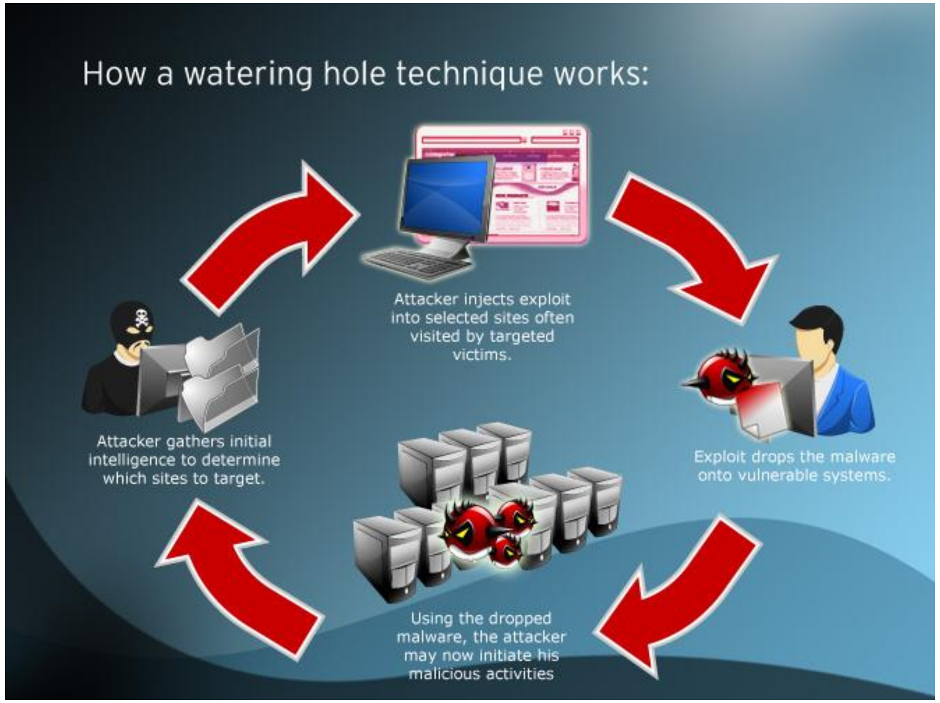
Zero-day

Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit.

Botnet Operation




Attacker
Bombs victim with HTTP requests
Legitimate requests can't get through and fail
User
Webserver

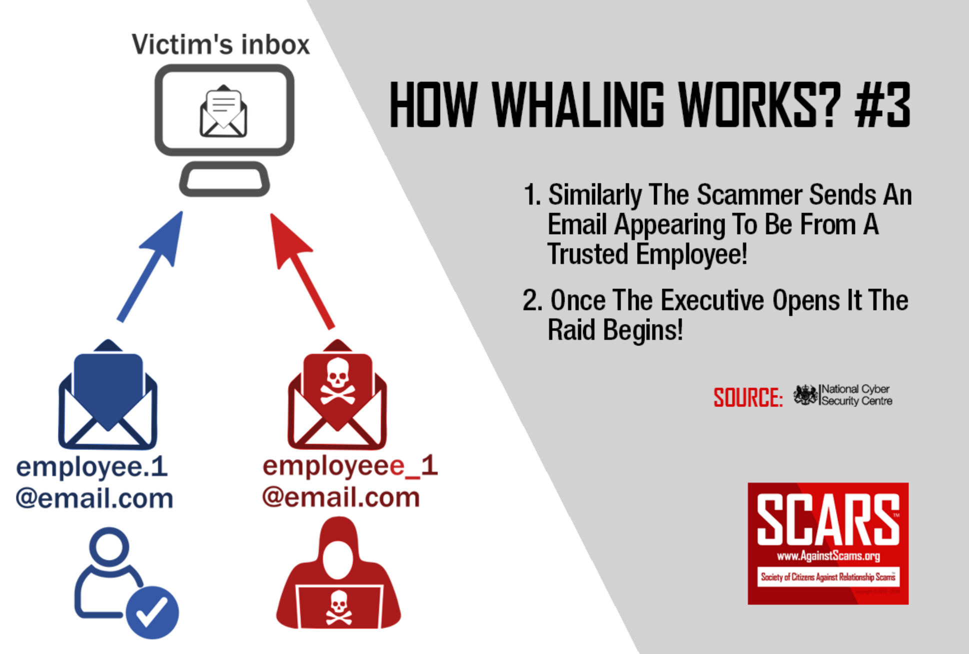

How a watering hole technique works:

Attacker gathers initial intelligence to determine which sites to target.

Attacker injects exploit into selected sites often visited by targeted victims.

Exploit drops the malware onto vulnerable systems.

Using the dropped malware, the attacker may now initiate his malicious activities

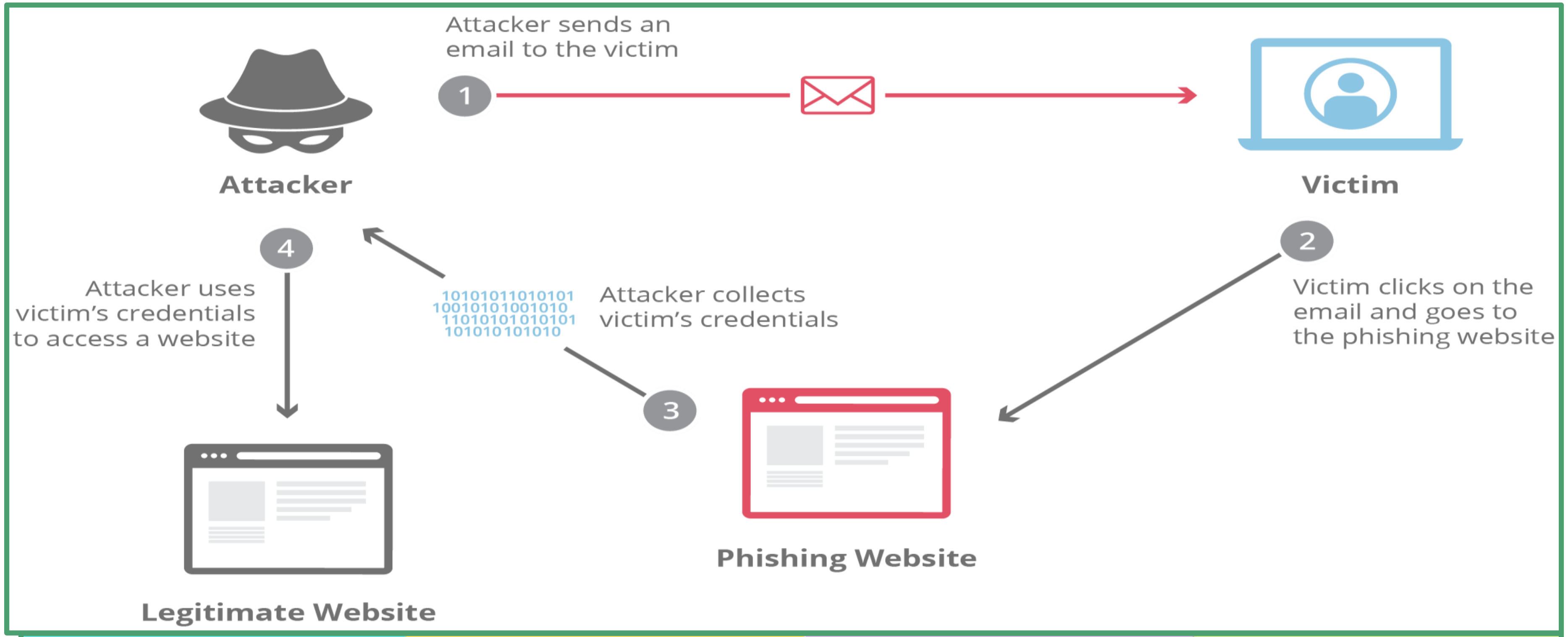


HOW WHALING WORKS? #3

1. Similarly The Scammer Sends An Email Appearing To Be From A Trusted Employee!
2. Once The Executive Opens It The Raid Begins!

SOURCE: National Cyber Security Centre

SCARS
www.AgainstScams.org
Society of Citizens Against Relationship Scams



Attacker

1 Attacker sends an email to the victim

Victim

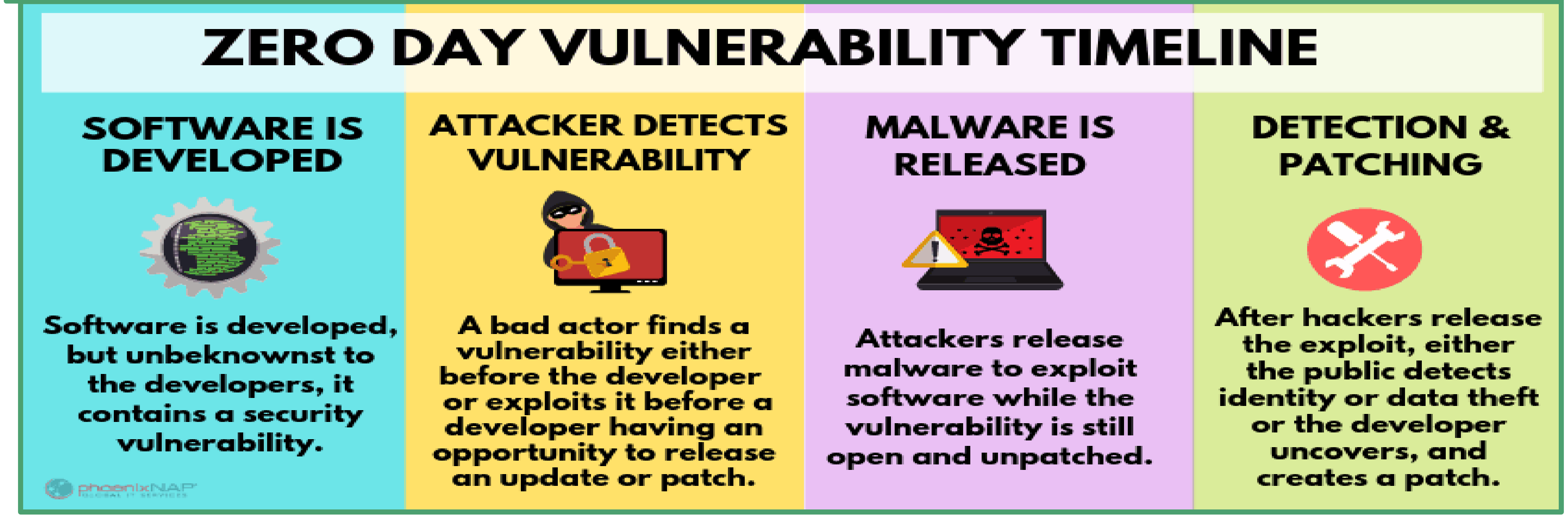
2 Victim clicks on the email and goes to the phishing website

Phishing Website

3 Attacker collects victim's credentials

4 Attacker uses victim's credentials to access a website

Legitimate Website



ZERO DAY VULNERABILITY TIMELINE

SOFTWARE IS DEVELOPED

Software is developed, but unbeknownst to the developers, it contains a security vulnerability.

ATTACKER DETECTS VULNERABILITY

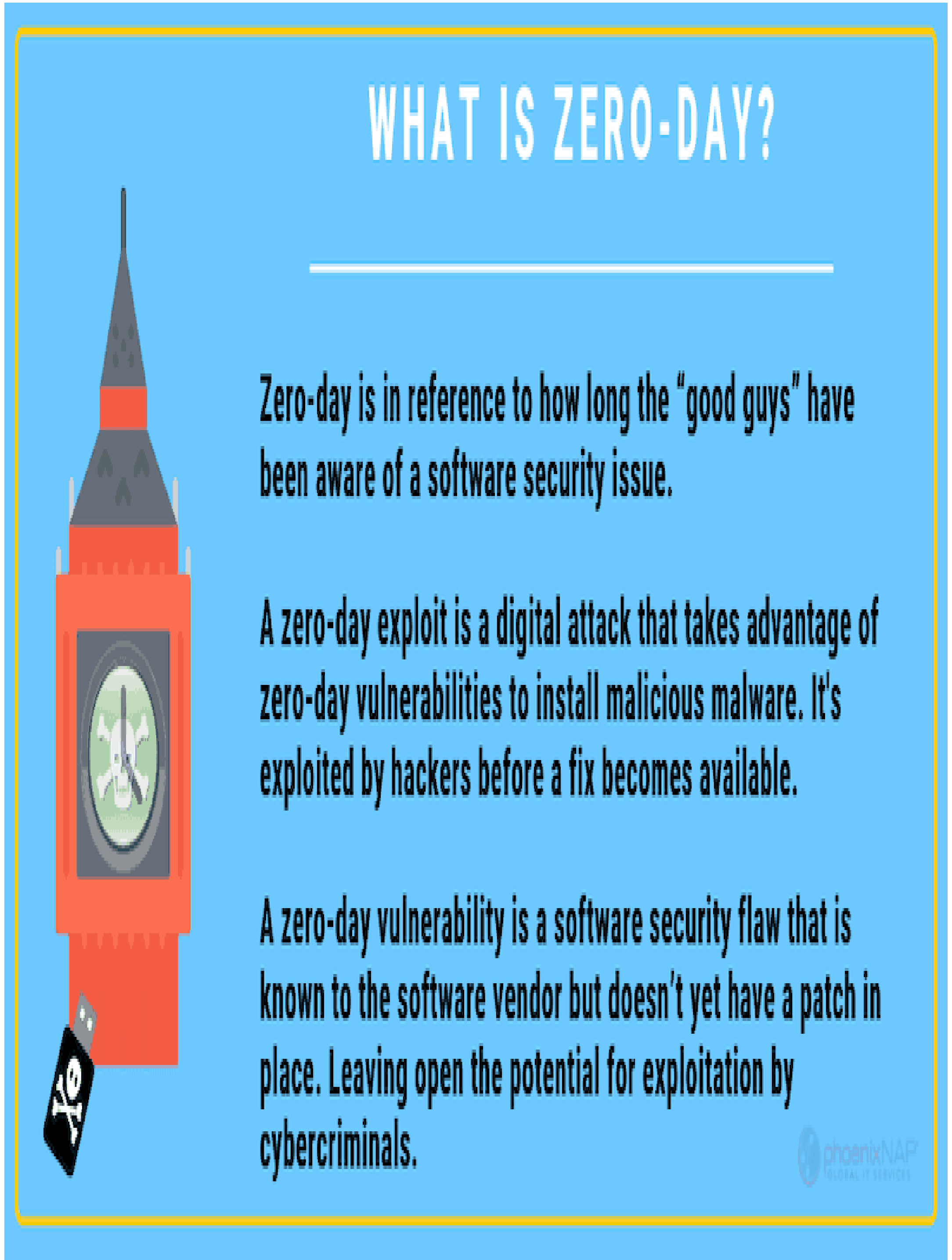
A bad actor finds a vulnerability either before the developer or exploits it before a developer having an opportunity to release an update or patch.

MALWARE IS RELEASED

Attackers release malware to exploit software while the vulnerability is still open and unpatched.

DETECTION & PATCHING

After hackers release the exploit, either the public detects identity or data theft or the developer uncovers, and creates a patch.

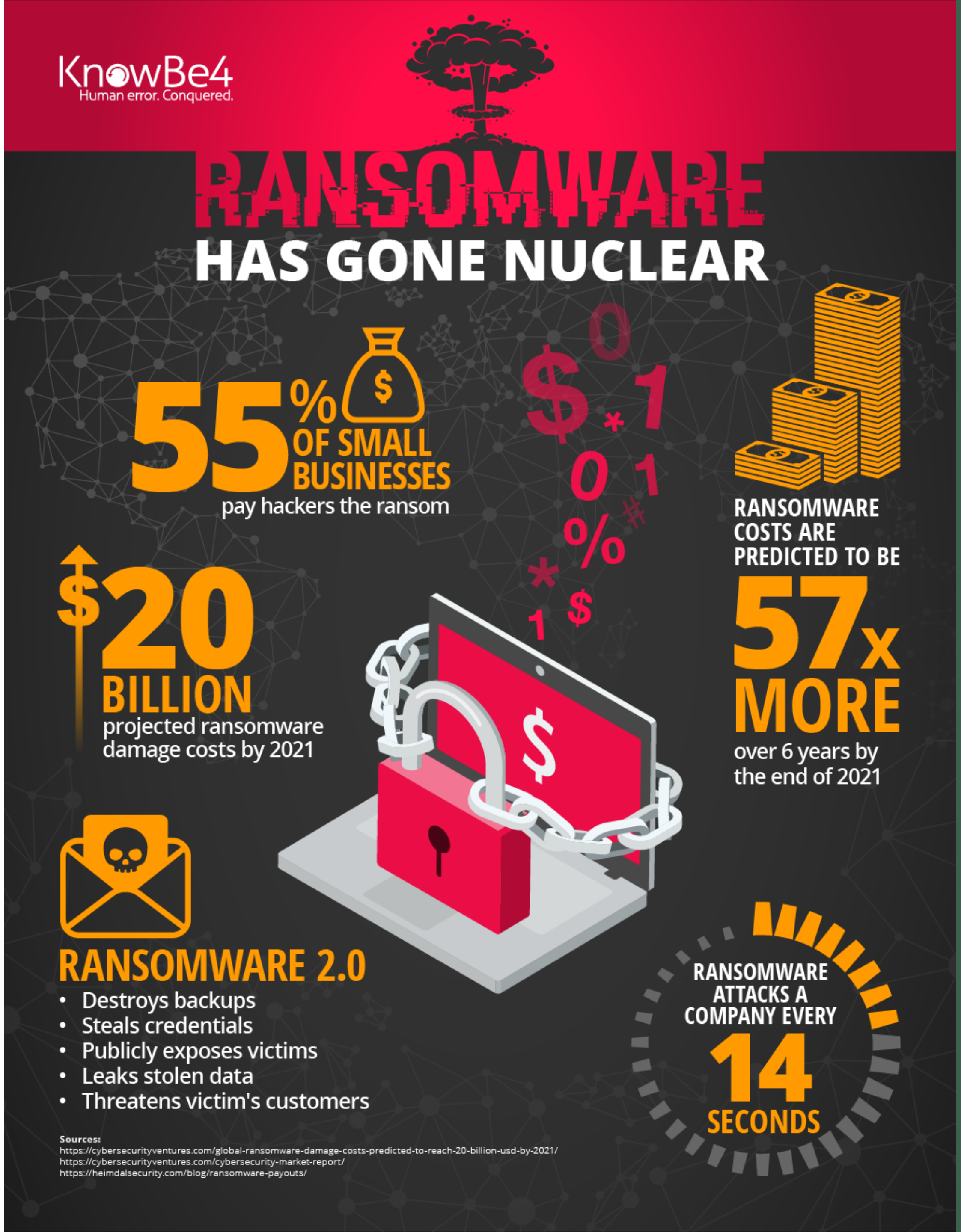


WHAT IS ZERO-DAY?

Zero-day is in reference to how long the "good guys" have been aware of a software security issue.

A zero-day exploit is a digital attack that takes advantage of zero-day vulnerabilities to install malicious malware. It's exploited by hackers before a fix becomes available.

A zero-day vulnerability is a software security flaw that is known to the software vendor but doesn't yet have a patch in place. Leaving open the potential for exploitation by cybercriminals.



KnowBe4
Human error. Conquered.

RANSOMWARE HAS GONE NUCLEAR

55% OF SMALL BUSINESSES pay hackers the ransom

$20 BILLION projected ransomware damage costs by 2021

RANSOMWARE COSTS ARE PREDICTED TO BE **57x MORE** over 6 years by the end of 2021

RANSOMWARE 2.0

- Destroys backups
- Steals credentials
- Publicly exposes victims
- Leaks stolen data
- Threatens victim's customers

RANSOMWARE ATTACKS A COMPANY EVERY **14 SECONDS**

Sources:
https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
https://cybersecurityventures.com/cybersecurity-market-report/
https://heimdalsecurity.com/blog/ransomware-payouts/

Introduction to Information Security

- **Security** can be defined as the degree of protection against criminal activity, danger, damage, and/or loss.
- **Information security** refers to all of the processes and policies designed to protect an organization's information and information systems (IS) from unauthorized access, use, disclosure, disruption, modification, or destruction.
- A **threat** to an information resource is any danger to which a system may be exposed.
- An information resource's **vulnerability** is the possibility that the system will be harmed by a threat.

Five key factors contributing to the increasing vulnerability of organizational information resources

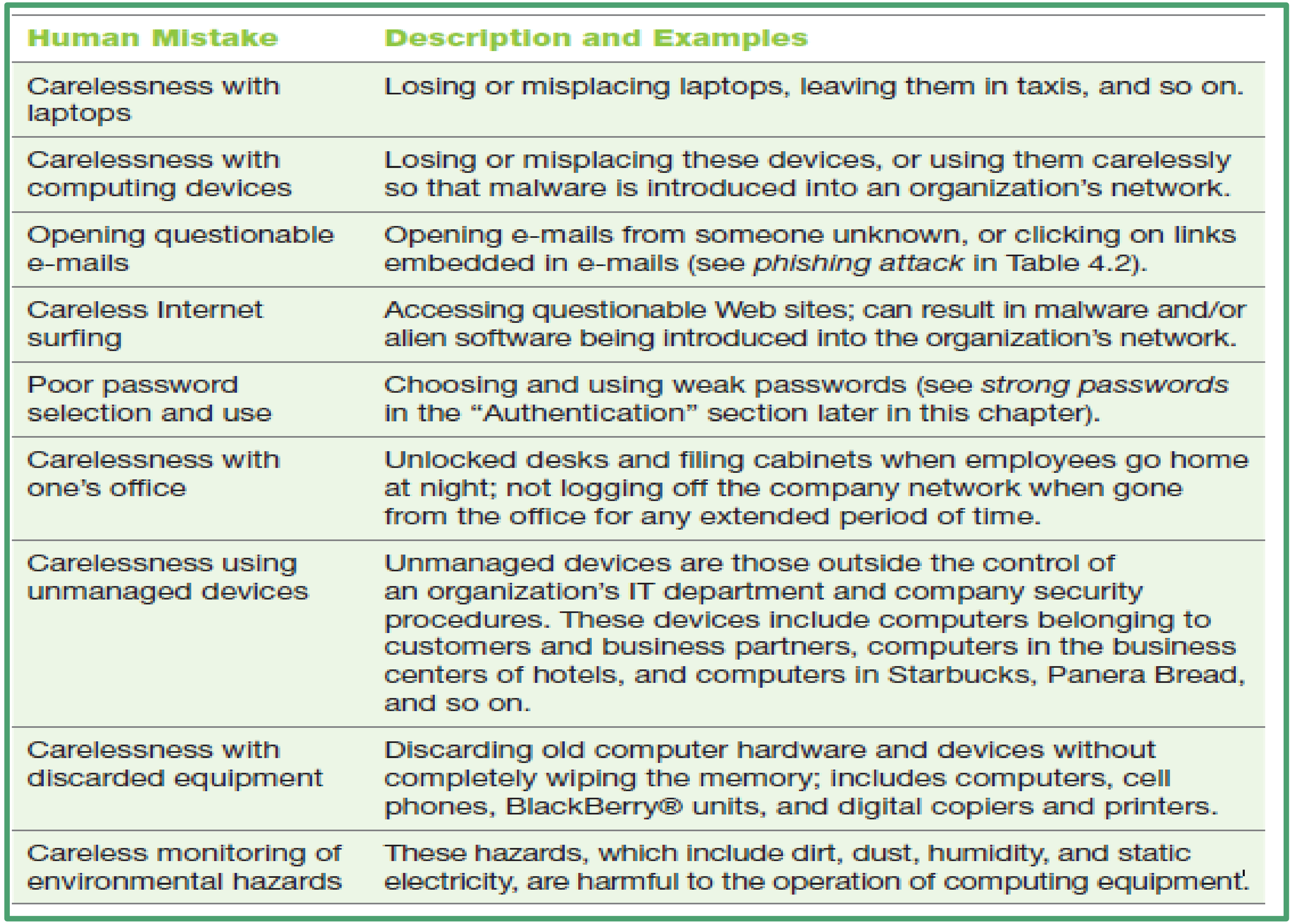
- Today’s interconnected, interdependent, wirelessly networked business environment;
- Smaller, faster, cheaper computers and storage devices;
- Decreasing skills necessary to be a computer hacker;
- International organized crime taking over cybercrime;
- Lack of management support

Above five key factors are contributing to the increasing vulnerability of organizational information resources, making it much more difficult to secure them

Threats to Information system

- The two major categories of threats are **unintentional threats** and **deliberate threats.**
- Unintentional threats are acts performed without malicious intent that nevertheless represent a serious threat to information security.
- A major category of unintentional threats is human error.
- Human errors or mistakes by employees pose a large problem as the result of laziness, carelessness, or a lack of awareness concerning information security.
- This lack of awareness comes from poor education and training efforts by the organization.

Human errors/mistakes



Human Mistake	Description and Examples
Carelessness with laptops	Losing or misplacing laptops, leaving them in taxis, and so on.
Carelessness with computing devices	Losing or misplacing these devices, or using them carelessly so that malware is introduced into an organization's network.
Opening questionable e-mails	Opening e-mails from someone unknown, or clicking on links embedded in e-mails (see *phishing attack* in Table 4.2).
Careless Internet surfing	Accessing questionable Web sites; can result in malware and/or alien software being introduced into the organization's network.
Poor password selection and use	Choosing and using weak passwords (see *strong passwords* in the "Authentication" section later in this chapter).
Carelessness with one's office	Unlocked desks and filing cabinets when employees go home at night; not logging off the company network when gone from the office for any extended period of time.
Carelessness using unmanaged devices	Unmanaged devices are those outside the control of an organization's IT department and company security procedures. These devices include computers belonging to customers and business partners, computers in the business centers of hotels, and computers in Starbucks, Panera Bread, and so on.
Carelessness with discarded equipment	Discarding old computer hardware and devices without completely wiping the memory; includes computers, cell phones, BlackBerry® units, and digital copiers and printers.
Careless monitoring of environmental hazards	These hazards, which include dirt, dust, humidity, and static electricity, are harmful to the operation of computing equipment.

Unintentional Threats to Information Systems

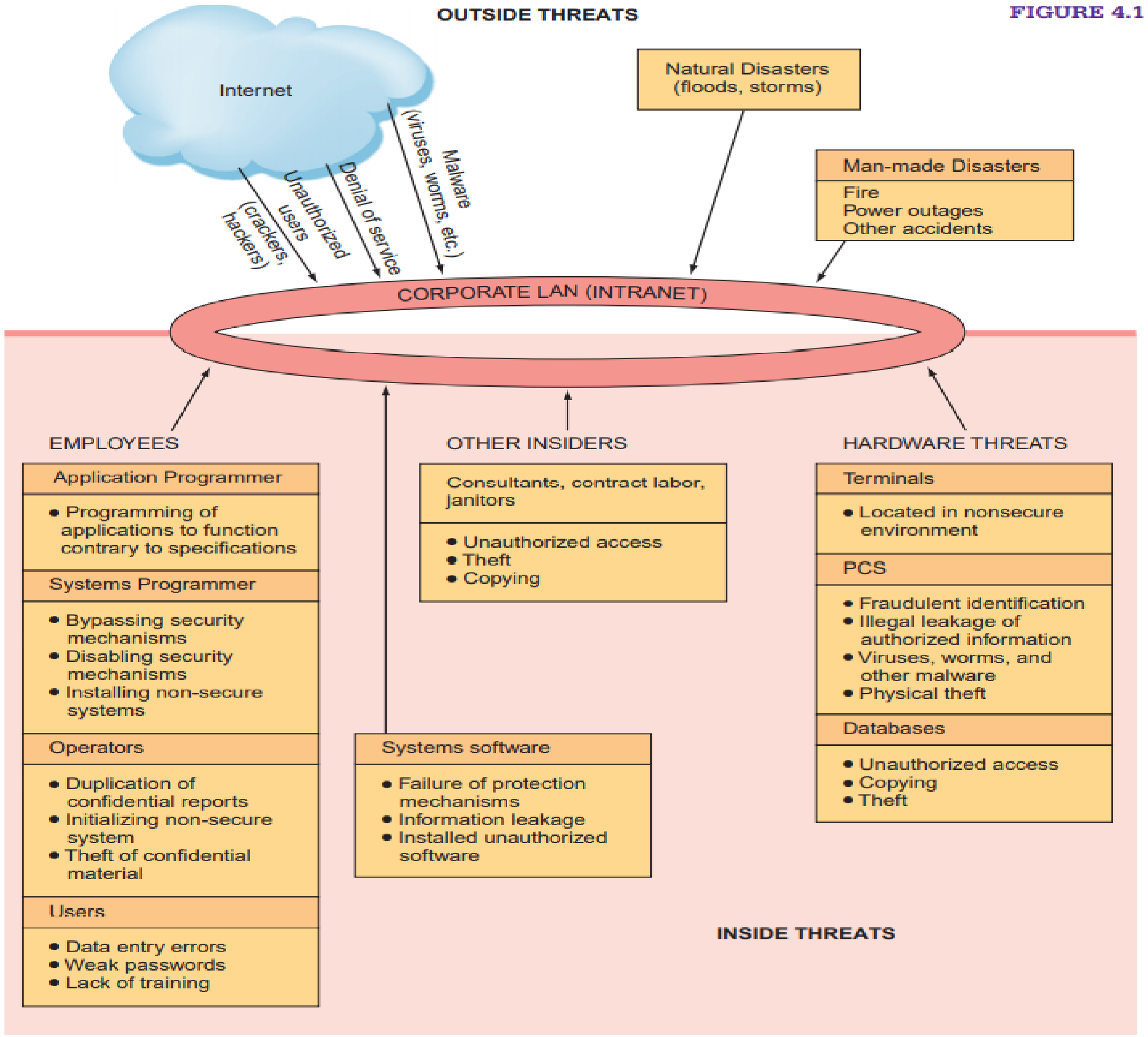


FIGURE 4.1 Security threats.

OUTSIDE THREATS

Internet

Unauthorized users (crackers, hackers)

Denial of service

Malware (viruses, worms, etc.)

Natural Disasters (floods, storms)

Man-made Disasters

- Fire
- Power outages
- Other accidents

CORPORATE LAN (INTRANET)

EMPLOYEES

Application Programmer

- Programming of applications to function contrary to specifications

Systems Programmer

- Bypassing security mechanisms
- Disabling security mechanisms
- Installing non-secure systems

Operators

- Duplication of confidential reports
- Initializing non-secure system
- Theft of confidential material

Users

- Data entry errors
- Weak passwords
- Lack of training

OTHER INSIDERS

Consultants, contract labor, janitors

- Unauthorized access
- Theft
- Copying

Systems software

- Failure of protection mechanisms
- Information leakage
- Installed unauthorized software

HARDWARE THREATS

Terminals

- Located in nonsecure environment

PCS

- Fraudulent identification
- Illegal leakage of authorized information
- Viruses, worms, and other malware
- Physical theft

Databases

- Unauthorized access
- Copying
- Theft

INSIDE THREATS

Deliberate Threats to Information Systems

- Spying or trespass
- Information extortion
- Sabotage or vandalism
- Theft of equipment or information
- Identity theft
- Compromises to intellectual property
- Software attacks
- Supervisory control and data acquisition (SCADA) attacks
- Cyberterrorism and cyberwarfare

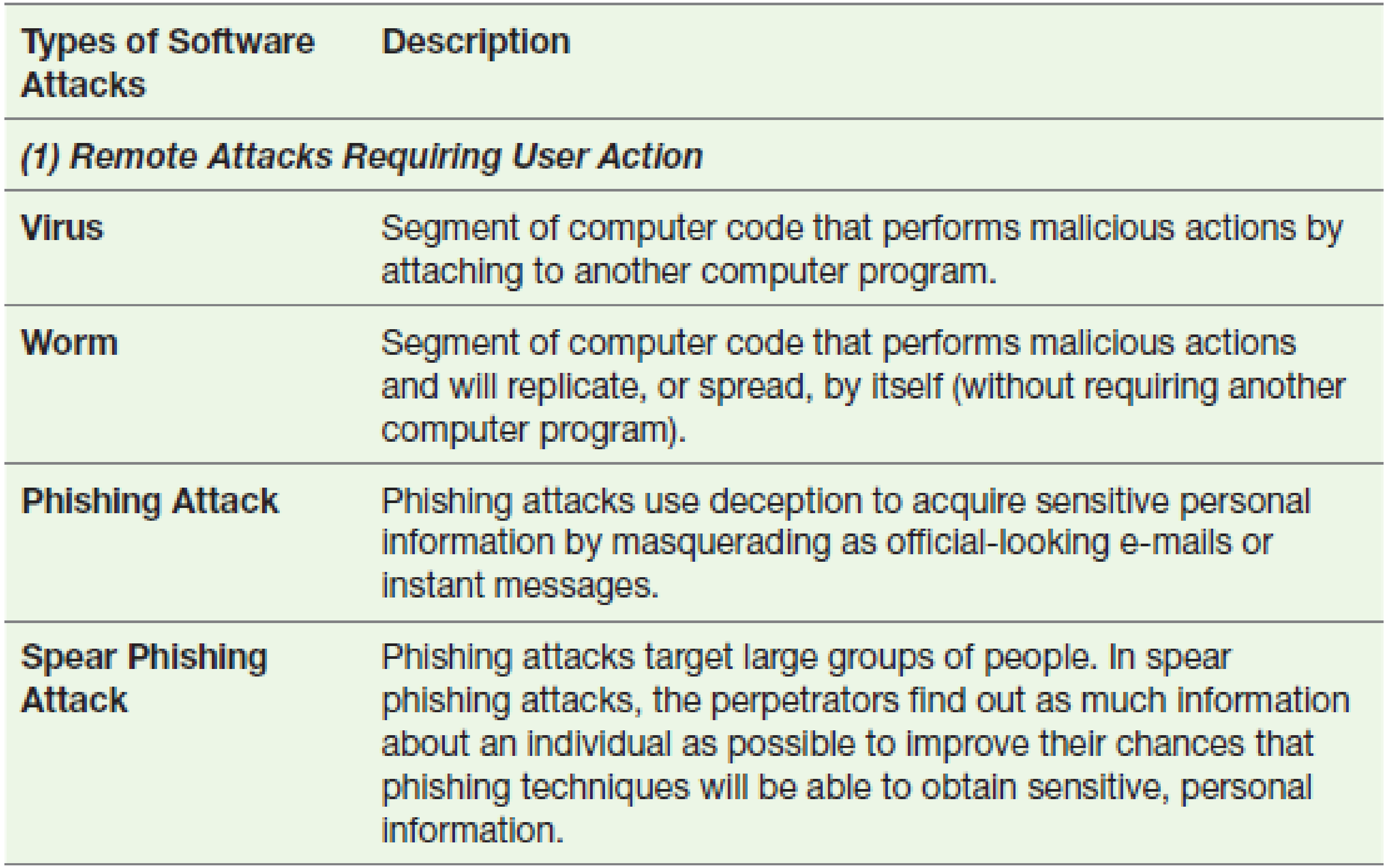
Deliberate Threats to Information Systems contd..

- Espionage or trespass occurs when an unauthorized individual attempts to gain illegal access to organizational information.
- Information extortion occurs when an attacker either threatens to steal, or actually steals, information from a company.
- Sabotage and vandalism are deliberate acts that involve defacing an organization’s Web site, possibly damaging the organization’s image and causing its customers to lose faith
- **Identity theft** is the deliberate assumption of another person’s identity, usually to gain access to his or her financial information or to frame him or her for a crime
- **Intellectual property** is the property created by individuals or corporations that is protected under *trade secret*, *patent*, and *copyright* laws.

Deliberate Threats to Information Systems
contd..

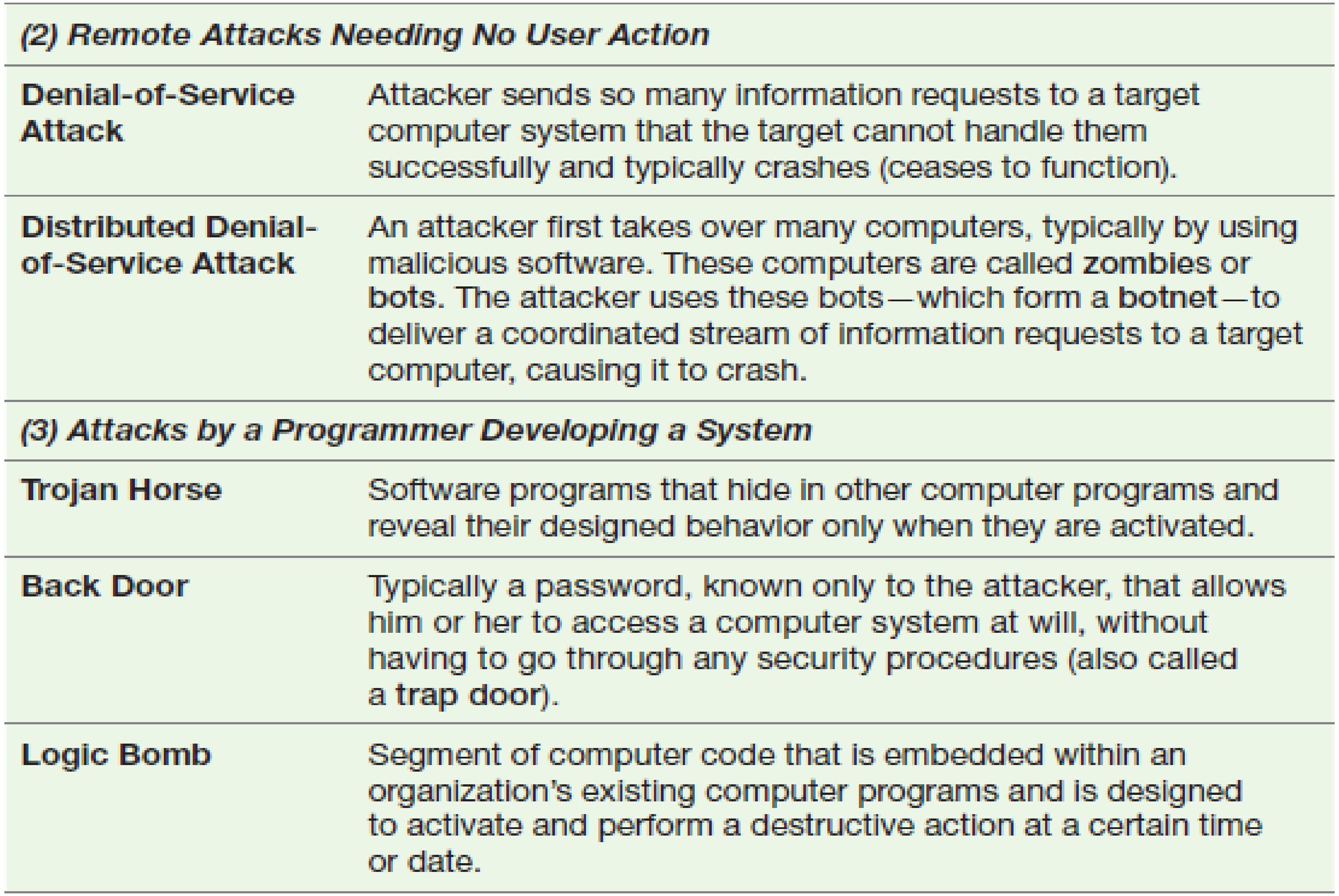
- Alien software is secret software that is installed on your computer through duplicitous methods. It can report on your Web surfing habits and other personal behavior
- SCADA systems are used to monitor or to control chemical, physical, and transport processes such as those used in oil refineries, water and sewage treatment plants, electrical generators, and nuclear power plants.
  - SCADA systems consist of multiple sensors, a master computer, and communications infrastructure.
  - If attackers gain access to the network, they can cause serious damage, such as disrupting the power grid over a large area or upsetting the operations of a large chemical or nuclear plant.
- **Cyberterrorism** and **cyberwarfare** refer to malicious acts in which attackers use a target’s computer systems, particularly via the Internet, to cause physical, real-world harm or severe disruption

Software Attacks



Types of Software Attacks	Description
(1) Remote Attacks Requiring User Action	
Virus	Segment of computer code that performs malicious actions by attaching to another computer program.
Worm	Segment of computer code that performs malicious actions and will replicate, or spread, by itself (without requiring another computer program).
Phishing Attack	Phishing attacks use deception to acquire sensitive personal information by masquerading as official-looking e-mails or instant messages.
Spear Phishing Attack	Phishing attacks target large groups of people. In spear phishing attacks, the perpetrators find out as much information about an individual as possible to improve their chances that phishing techniques will be able to obtain sensitive, personal information.

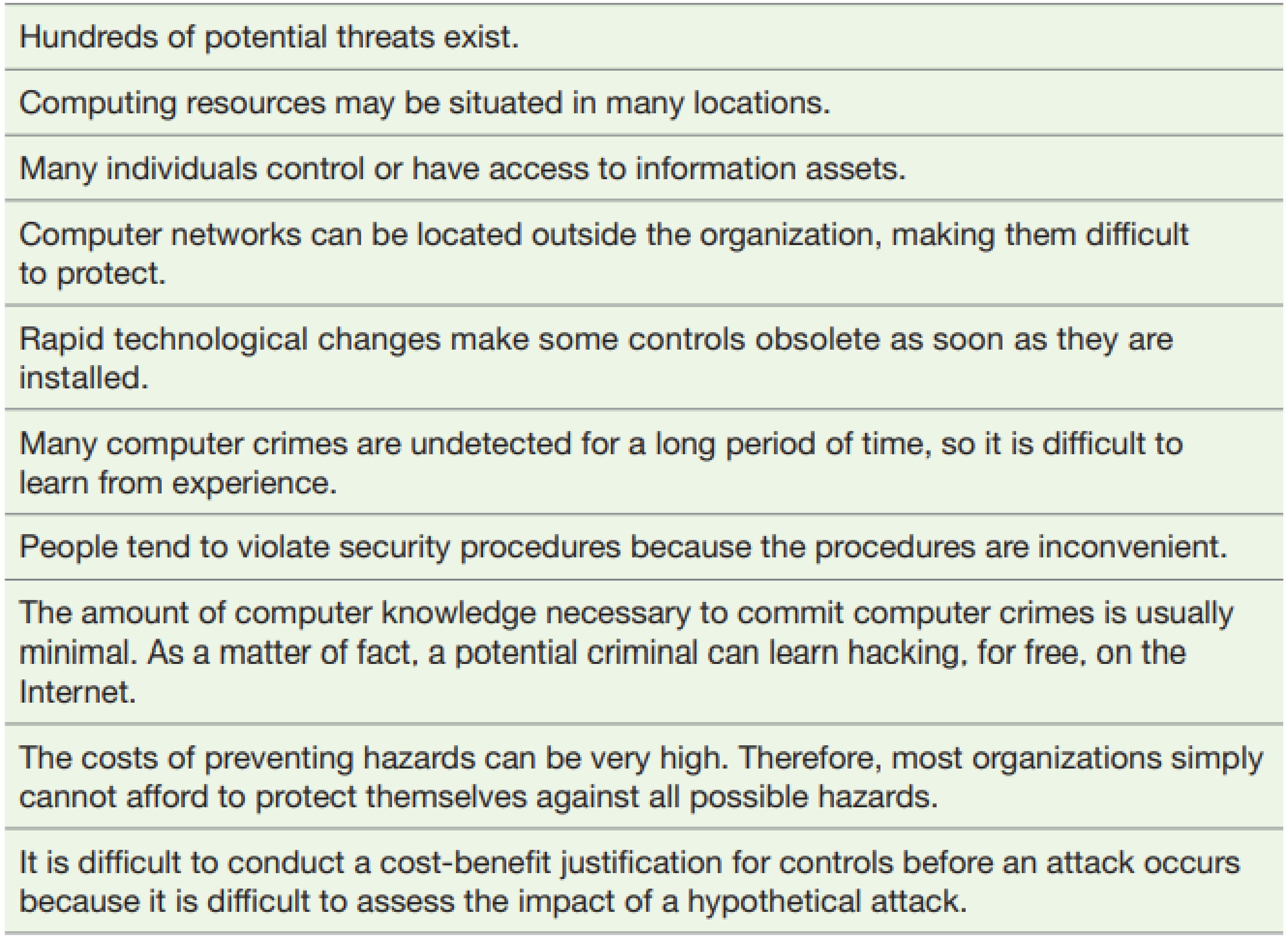
Software Attacks



(2) Remote Attacks Needing No User Action	
Denial-of-Service Attack	Attacker sends so many information requests to a target computer system that the target cannot handle them successfully and typically crashes (ceases to function).
Distributed Denial-of-Service Attack	An attacker first takes over many computers, typically by using malicious software. These computers are called **zombies** or **bots**. The attacker uses these bots—which form a **botnet**—to deliver a coordinated stream of information requests to a target computer, causing it to crash.
(3) Attacks by a Programmer Developing a System	
Trojan Horse	Software programs that hide in other computer programs and reveal their designed behavior only when they are activated.
Back Door	Typically a password, known only to the attacker, that allows him or her to access a computer system at will, without having to go through any security procedures (also called a **trap door**).
Logic Bomb	Segment of computer code that is embedded within an organization's existing computer programs and is designed to activate and perform a destructive action at a certain time or date.

What Organizations Are Doing to Protect Information Resources?

Why it is difficult to protect information

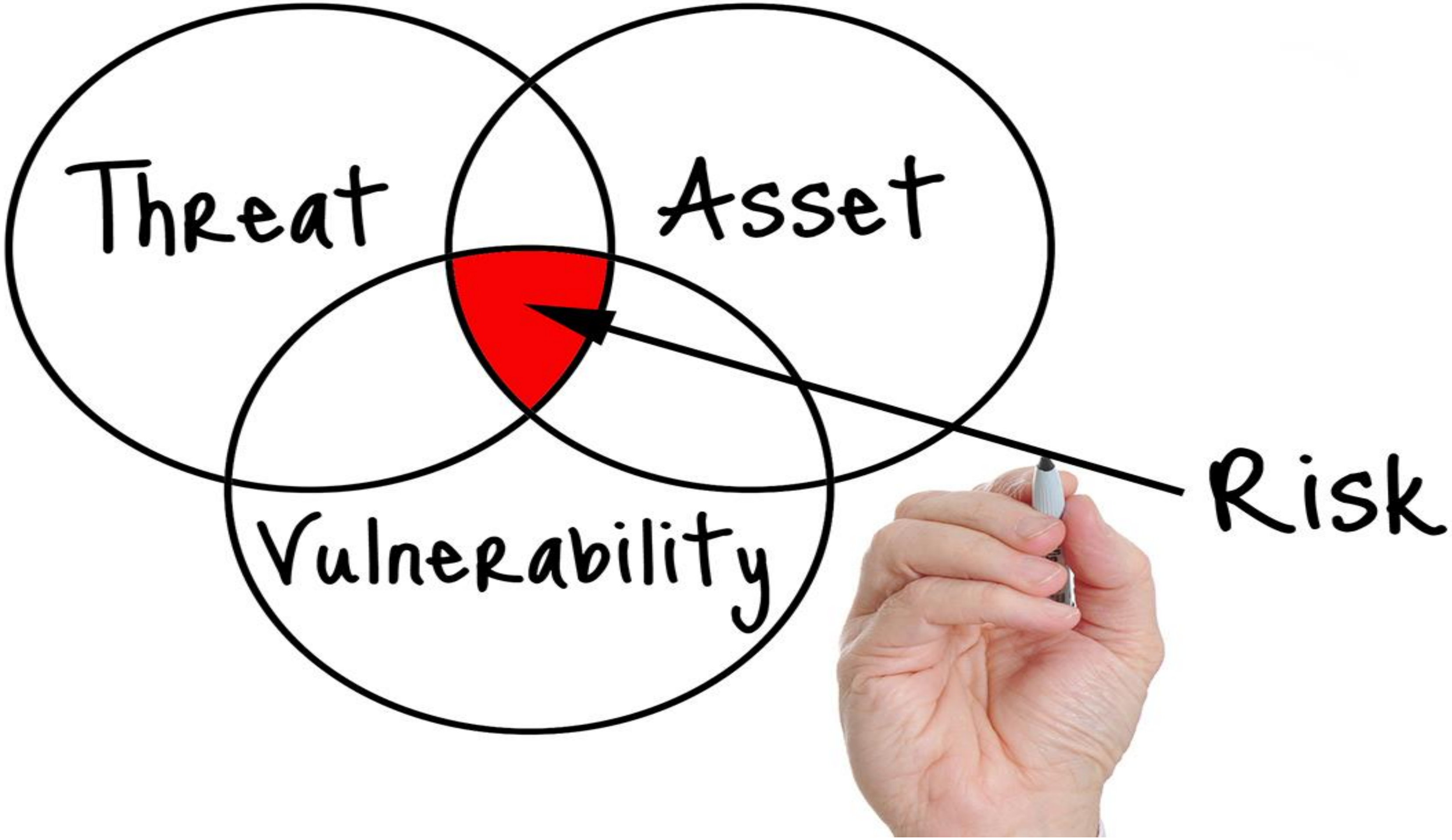


Hundreds of potential threats exist.
Computing resources may be situated in many locations.
Many individuals control or have access to information assets.
Computer networks can be located outside the organization, making them difficult to protect.
Rapid technological changes make some controls obsolete as soon as they are installed.
Many computer crimes are undetected for a long period of time, so it is difficult to learn from experience.
People tend to violate security procedures because the procedures are inconvenient.
The amount of computer knowledge necessary to commit computer crimes is usually minimal. As a matter of fact, a potential criminal can learn hacking, for free, on the Internet.
The costs of preventing hazards can be very high. Therefore, most organizations simply cannot afford to protect themselves against all possible hazards.
It is difficult to conduct a cost-benefit justification for controls before an attack occurs because it is difficult to assess the impact of a hypothetical attack.

What Organizations Are Doing to Protect Information Resources?

- Organizations spend a great deal of time and money protecting their information resources.
- Before doing so, they perform **risk management**.
- A **risk** is the probability that a threat will impact an information resource.
- The goal of **risk management** is to identify, control, and minimize the impact of threats.
- Risk management consists of three processes: risk analysis, risk mitigation, and controls evaluation.

Why Risk management?



1.Risk analysis

Organizations perform risk analyses to ensure that their IS security programs are cost effective.

Risk analysis involves three steps:

(1) assessing the value of each asset being protected,

(2) estimating the probability that each asset will be compromised,

(3) comparing the probable costs of the asset’s being compromised with the costs of protecting that asset.

The organization then considers how to mitigate the risk.

2. Risk mitigation

In **risk mitigation**, the organization takes concrete actions against risks.

- Risk mitigation has two functions:

  (1) implementing controls to prevent identified threats from occurring,

  (2) developing a means of recovery if the threat becomes a reality.

- There are several risk mitigation strategies that organizations can adopt.
- The three most common are risk acceptance, risk limitation, and risk transference.
- **Risk acceptance**: Accept the potential risk, continue operating with no controls, and absorb any damages that occur.
- **Risk limitation**: Limit the risk by implementing controls that minimize the impact of the threat.
- **Risk transference**: Transfer the risk by using other means to compensate for the loss, such as by purchasing insurance.

3. Controls evaluation

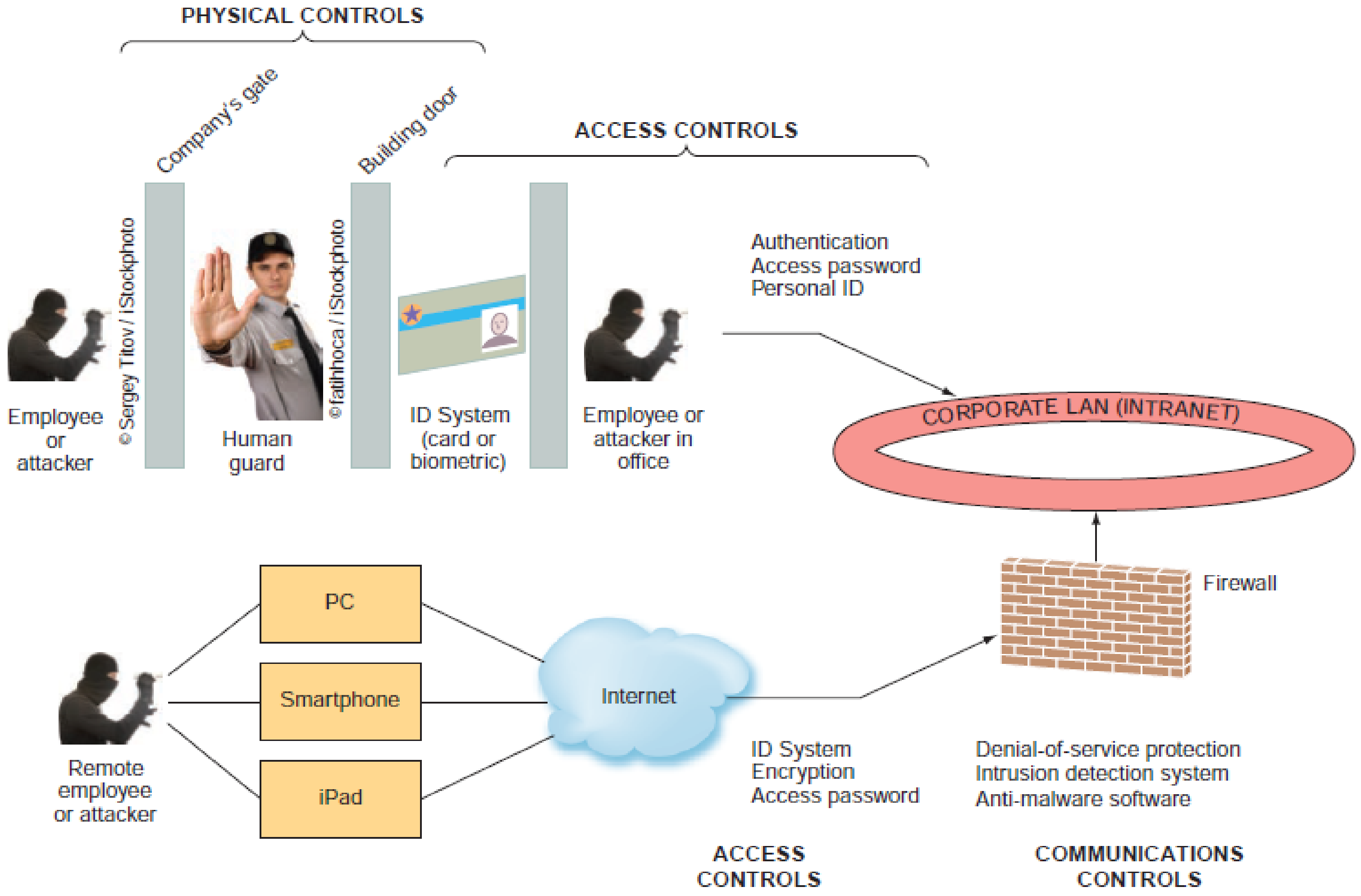
- Finally, in controls evaluation, the organization examines the costs of implementing adequate control measures against the value of those control measures.

- If the costs of implementing a control are greater than the value of the asset being protected, the control is not cost effective

Information Security Controls

- To protect their information assets, organizations implement **controls**, or defense mechanisms (also called *countermeasures*).
- These controls are designed to protect all of the components of an information system, including data, software, hardware, and networks.
- Controls are intended to prevent accidental hazards, detect intentional acts, detect problems as early as possible, enhance damage recovery, and correct problems
- Three major types of controls:
  1. Physical controls
  2. Access controls
  3. Communications controls/ Network controls

Information Security Controls



Physical controls

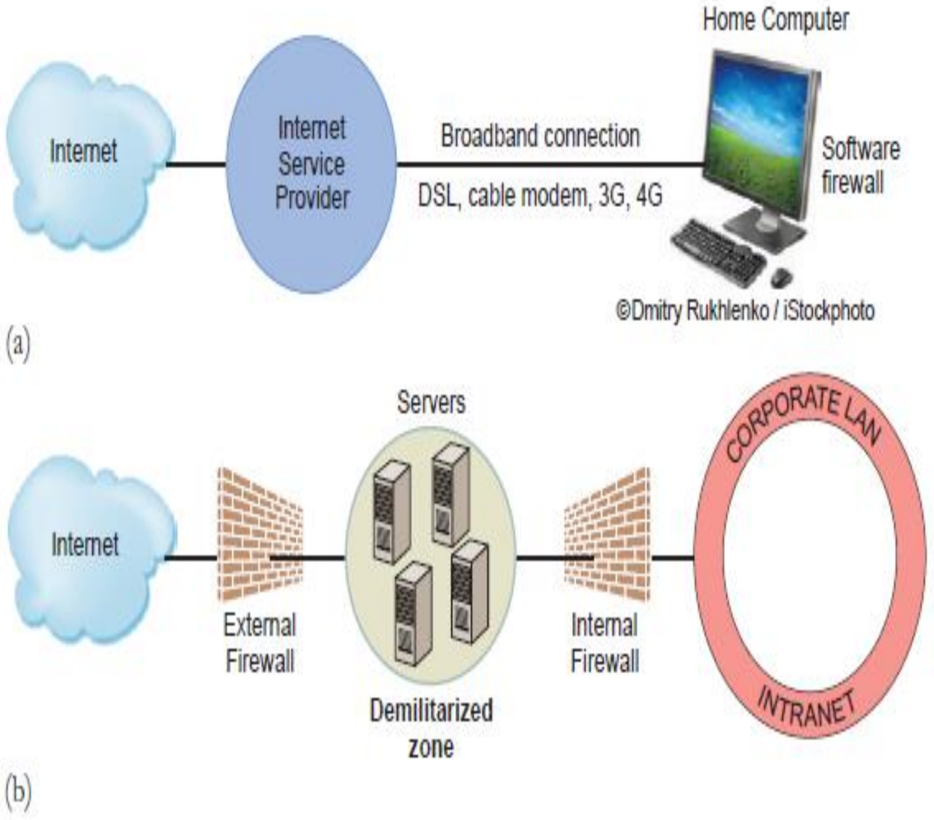
- **Physical controls** prevent unauthorized individuals from gaining access to a company's facilities.
- Common physical controls include walls, doors, fencing, gates, locks, badges, guards, and alarm systems.
- More sophisticated physical controls include pressure sensors, temperature sensors, and motion detectors.
- Organizations also implement physical security measures that limit computer users to acceptable login times and locations.

Access controls

- **Access controls** restrict unauthorized individuals from using information resources.
- These controls involve two major functions:
  - Authentication and authorization.
- **Authentication** confirms the identity of the person requiring access. After the person is authenticated (identified), the next step is authorization.
- **Authorization** determines which actions, rights, or privileges the person has, based on his or her verified identity.

Communications controls

- **Communications controls** (also called **network controls**) secure the movement of data across networks.
- Communications controls consist of firewalls, anti-malware systems, whitelisting and blacklisting, encryption, virtual private networks (VPNs), secure socket layer (SSL), and employee monitoring systems



Communications controls contd..

- A **Firewall** is a system that prevents a specific type of information from moving between untrusted networks, such as the Internet, and private networks, such as your company’s network

- **Anti-malware systems**, also called *antivirus*, or *AV*, software, are software packages that attempt to identify and eliminate viruses and worms, and other malicious software

Communications controls contd..

- Whitelisting is a process in which a company identifies the software that it will allow to run on its computers.
  - Whitelisting permits acceptable software to run, and it either prevents any other software from running or it lets new software run in a quarantined environment until the company can verify its validity.
- **Blacklisting** allows everything to run unless it is on the blacklist. A blacklist, then, includes certain types of software that are not allowed to run in the company environment.
  - For example, a company might blacklist peer-to-peer file sharing on its systems.
  - In addition to software, people, devices, and Web sites can also be whitelisted and blacklisted.

Communications controls contd..

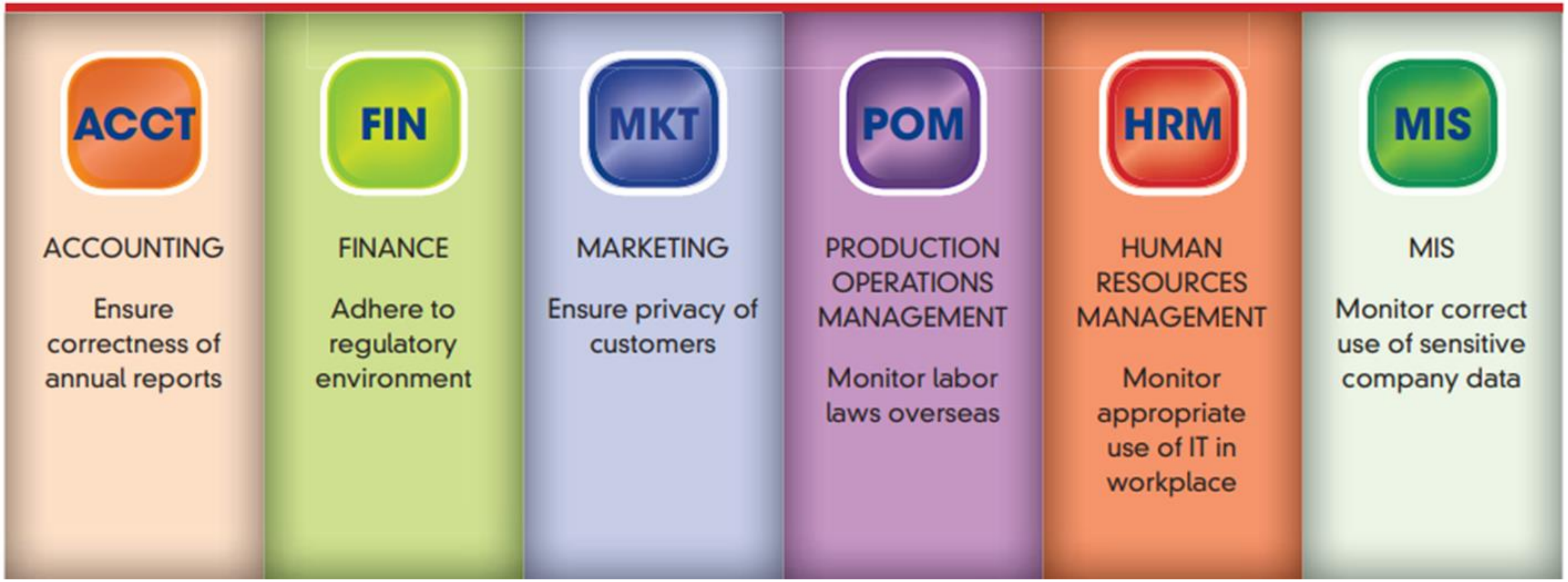
- **Encryption** is the process of converting an original message into a form that cannot be read by anyone except the intended receiver.
  - The majority of encryption systems use public-key encryption.
- A third party, called a **certificate authority**, acts as a trusted intermediary between the companies.
  - The certificate authority issues digital certificates and verifies the integrity of the certificates.
- A **virtual private network** is a private network that uses a public network (usually the Internet) to connect users.
  - They are created by using log-ins, encryption, and other techniques to enhance the user's **privacy**.
- **Secure socket layer**, now called **transport layer security (TLS)**, is an encryption standard used for secure transactions such as credit card purchases and online banking.
  - TLS encrypts and decrypts data between a Web server and a browser end to end
- **Employee monitoring systems**, monitor their employees' computers, e-mail activities, and Internet surfing activities.

Ethics and Privacy

Contents…

› Ethical Issues

› Privacy



ACCT	FIN	MKT	POM	HRM	MIS
ACCOUNTING	FINANCE	MARKETING	PRODUCTION OPERATIONS MANAGEMENT	HUMAN RESOURCES MANAGEMENT	MIS
Ensure correctness of annual reports	Adhere to regulatory environment	Ensure privacy of customers	Monitor labor laws overseas	Monitor appropriate use of IT in workplace	Monitor correct use of sensitive company data

Ethical Issues

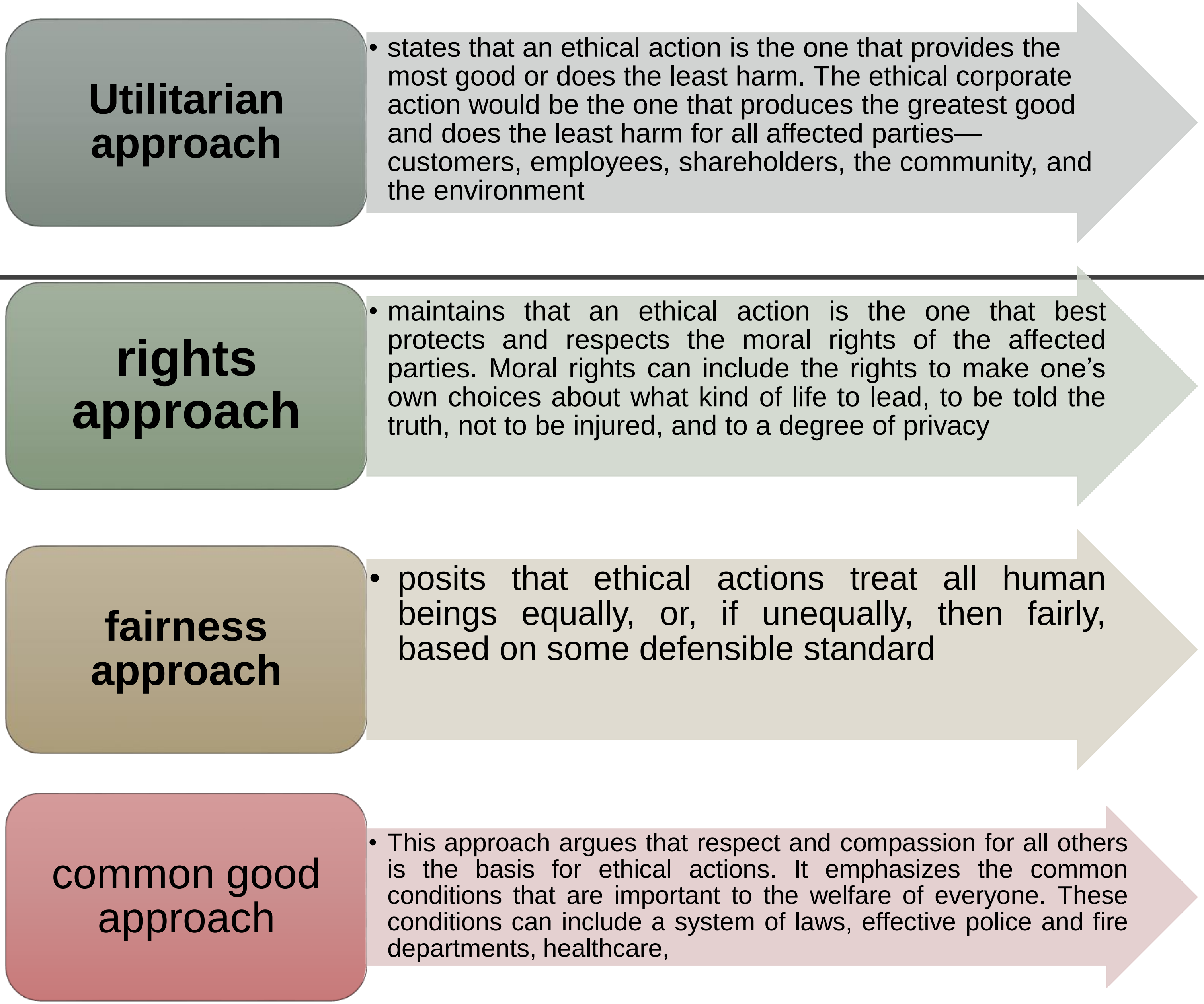
- Ethical Frameworks
- Ethics in the Corporate Environment
- Ethics and Information Technology

Ethical Frameworks

- Utilitarian Approach
- Rights Approach
- Fairness Approach
- Common Good Approach
- Five Steps of the General Ethical Framework

Utilitarian Approach

- Ethics refers to the principles of right and wrong that individuals use to make choices that guide their behavior. Deciding what is right or wrong is not always easy or clear cut.



Utilitarian approach

- states that an ethical action is the one that provides the most good or does the least harm. The ethical corporate action would be the one that produces the greatest good and does the least harm for all affected parties—customers, employees, shareholders, the community, and the environment

rights approach

- maintains that an ethical action is the one that best protects and respects the moral rights of the affected parties. Moral rights can include the rights to make one’s own choices about what kind of life to lead, to be told the truth, not to be injured, and to a degree of privacy

fairness approach

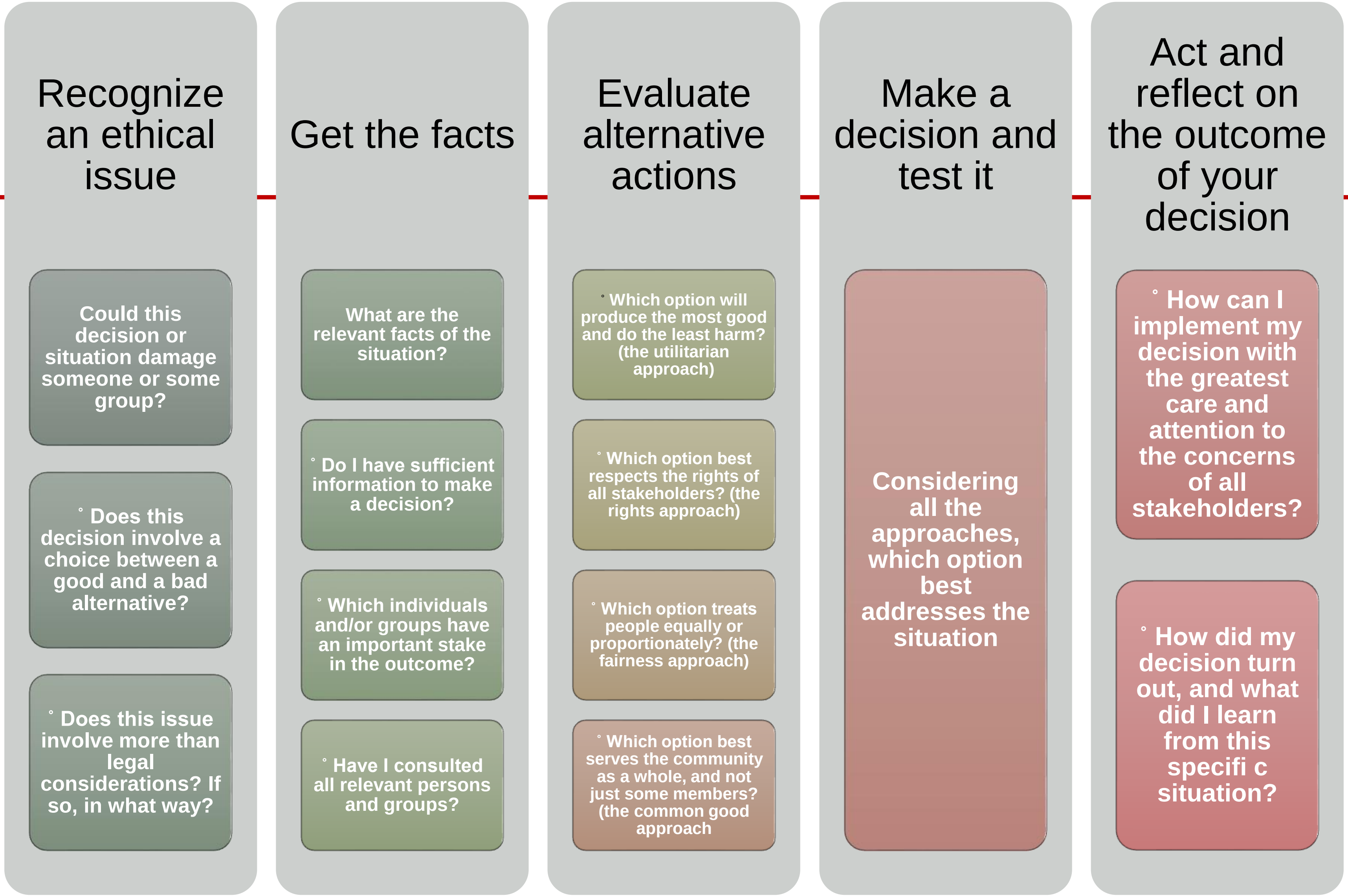
- posits that ethical actions treat all human beings equally, or, if unequally, then fairly, based on some defensible standard

common good approach

- This approach argues that respect and compassion for all others is the basis for ethical actions. It emphasizes the common conditions that are important to the welfare of everyone. These conditions can include a system of laws, effective police and fire departments, healthcare,

Five Steps of the General Ethical Framework

1. Recognize the Issue
2. Get the Facts
3. Evaluate Alternative Actions
4. Make a Decision and Test It
5. Act and Reflect on the Outcome of Your Decision



Recognize an ethical issue

- Could this decision or situation damage someone or some group?
- Does this decision involve a choice between a good and a bad alternative?
- Does this issue involve more than legal considerations? If so, in what way?

Get the facts

- What are the relevant facts of the situation?
- Do I have sufficient information to make a decision?
- Which individuals and/or groups have an important stake in the outcome?
- Have I consulted all relevant persons and groups?

Evaluate alternative actions

- Which option will produce the most good and do the least harm? (the utilitarian approach)
- Which option best respects the rights of all stakeholders? (the rights approach)
- Which option treats people equally or proportionately? (the fairness approach)
- Which option best serves the community as a whole, and not just some members? (the common good approach

Make a decision and test it

- Considering all the approaches, which option best addresses the situation

Act and reflect on the outcome of your decision

- How can I implement my decision with the greatest care and attention to the concerns of all stakeholders?
- How did my decision turn out, and what did I learn from this specific situation?

Ethics in the Corporate Environment

- Code of Ethics : it is a collection of principles intended to guide decision making by members of the organization
- Fundamental Tenets/views of Ethics
  - Responsibility: means that you accept the consequences of your decisions and actions.
  - Accountability : refers to determining who is responsible for actions that were taken
  - Liability : it is a legal concept that gives individuals the right to recover the damages done to them by other individuals,

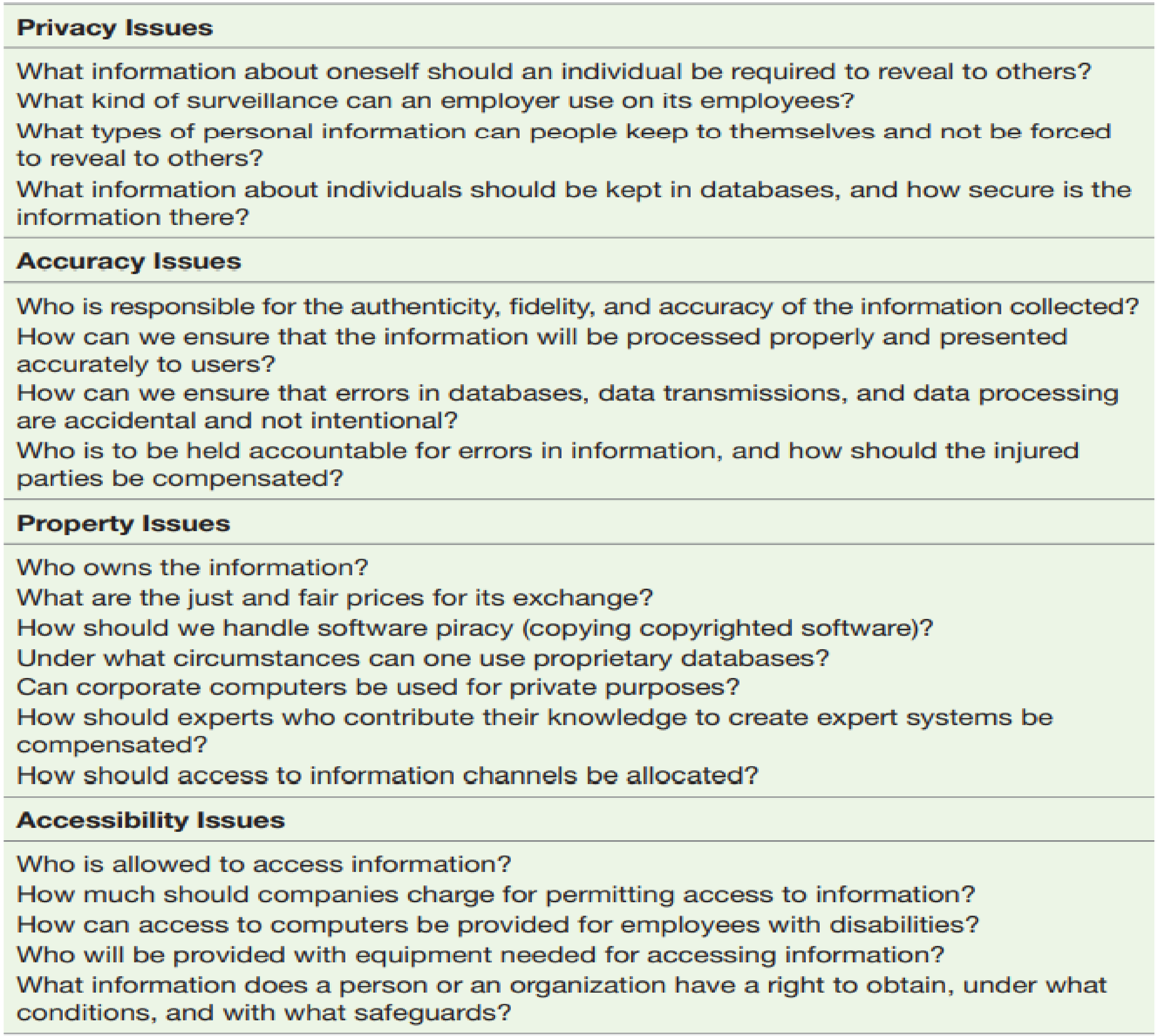
    organizations, or systems.

Ethics and Information Technology

- Should organizations monitor employees’ Web surfing and e-mail?
- • Should organizations sell customer information to other companies?
- • Should organizations audit employees’ computers for unauthorized software or illegally downloaded music or video files?

Ethics and Information Technology

- Privacy Issues: involve collecting, storing, and disseminating information about individuals.
- Accuracy Issues: involve the authenticity, reliability, and correctness of information that is collected and processed
- Property Issues : involve the ownership and value of information.
- Accessibility Issues revolve around who should have access to information and whether a fee should be paid for this access



Privacy Issues

What information about oneself should an individual be required to reveal to others?
What kind of surveillance can an employer use on its employees?
What types of personal information can people keep to themselves and not be forced to reveal to others?
What information about individuals should be kept in databases, and how secure is the information there?

Accuracy Issues

Who is responsible for the authenticity, fidelity, and accuracy of the information collected?
How can we ensure that the information will be processed properly and presented accurately to users?
How can we ensure that errors in databases, data transmissions, and data processing are accidental and not intentional?
Who is to be held accountable for errors in information, and how should the injured parties be compensated?

Property Issues

Who owns the information?
What are the just and fair prices for its exchange?
How should we handle software piracy (copying copyrighted software)?
Under what circumstances can one use proprietary databases?
Can corporate computers be used for private purposes?
How should experts who contribute their knowledge to create expert systems be compensated?
How should access to information channels be allocated?

Accessibility Issues

Who is allowed to access information?
How much should companies charge for permitting access to information?
How can access to computers be provided for employees with disabilities?
Who will be provided with equipment needed for accessing information?
What information does a person or an organization have a right to obtain, under what conditions, and with what safeguards?

Privacy

- In general, privacy is the right to be left alone and to be free of unreasonable personal intrusions. Information privacy is the right to determine when, and to what extent, information about you can be gathered and/or communicated to others. Privacy rights apply to individuals, groups, and institutions.

Privacy

- Electronic Surveillance
- Personal Information in Databases
- Information on Internet Bulletin Boards, Newsgroups, and Social Networking Sites
- Privacy Codes and Policies
- International Aspects of Privacy

Privacy: Two Rules

- Court decisions in many countries have generally followed two rules
  1. The right to privacy is not absolute. Privacy must be balanced against the needs of society.
  2. The public’s right to know replaces the individual’s right to privacy.

Electronic Surveillance

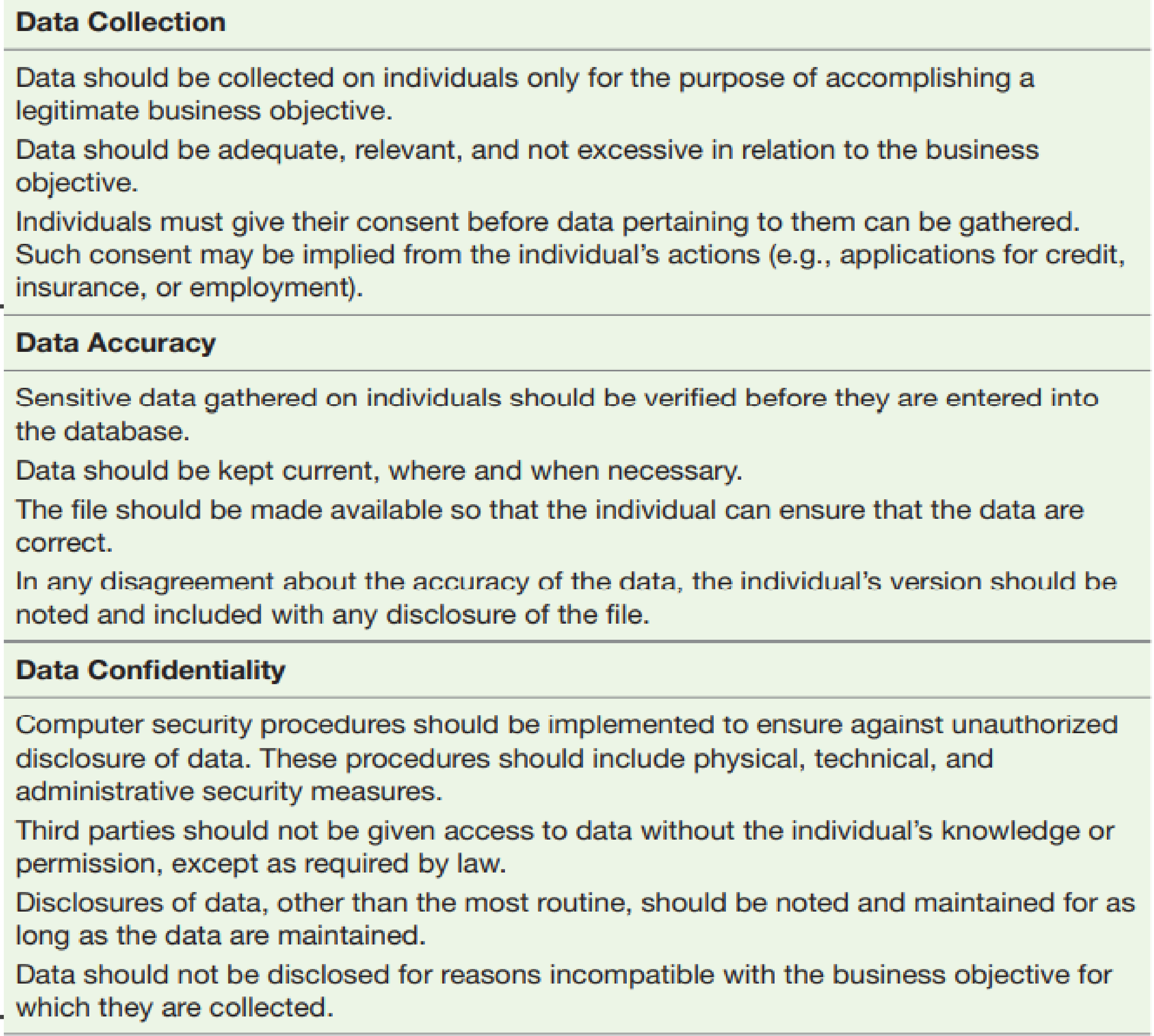
- According to the American Civil Liberties Union ACLU – Electronic surveillance is rapidly increasing
- Emerging Technologies increase monitoring of human activity
  - Your Smart Phone has become a Sensor
- Facial Recognition by Google & Facebook
- Tagging (Photos & Geo tagging)

Personal Information in Databases

- Major Concerns:
  - Do you know where the records are?
  - Are the records accurate?
  - Can you change inaccurate data?
  - How long will it take to make a change?
  - Under what circumstances will the personal data be released?

Personal Information in Databases (continued)

- Major Concerns:
  - How are the data used?
  - To whom are the data given or sold?
  - How secure are the data against access by unauthorized people?



Data Collection

Data should be collected on individuals only for the purpose of accomplishing a legitimate business objective.

Data should be adequate, relevant, and not excessive in relation to the business objective.

Individuals must give their consent before data pertaining to them can be gathered. Such consent may be implied from the individual's actions (e.g., applications for credit, insurance, or employment).

Data Accuracy

Sensitive data gathered on individuals should be verified before they are entered into the database.

Data should be kept current, where and when necessary.

The file should be made available so that the individual can ensure that the data are correct.

In any disagreement about the accuracy of the data, the individual's version should be noted and included with any disclosure of the file.

Data Confidentiality

Computer security procedures should be implemented to ensure against unauthorized disclosure of data. These procedures should include physical, technical, and administrative security measures.

Third parties should not be given access to data without the individual's knowledge or permission, except as required by law.

Disclosures of data, other than the most routine, should be noted and maintained for as long as the data are maintained.

Data should not be disclosed for reasons incompatible with the business objective for which they are collected.

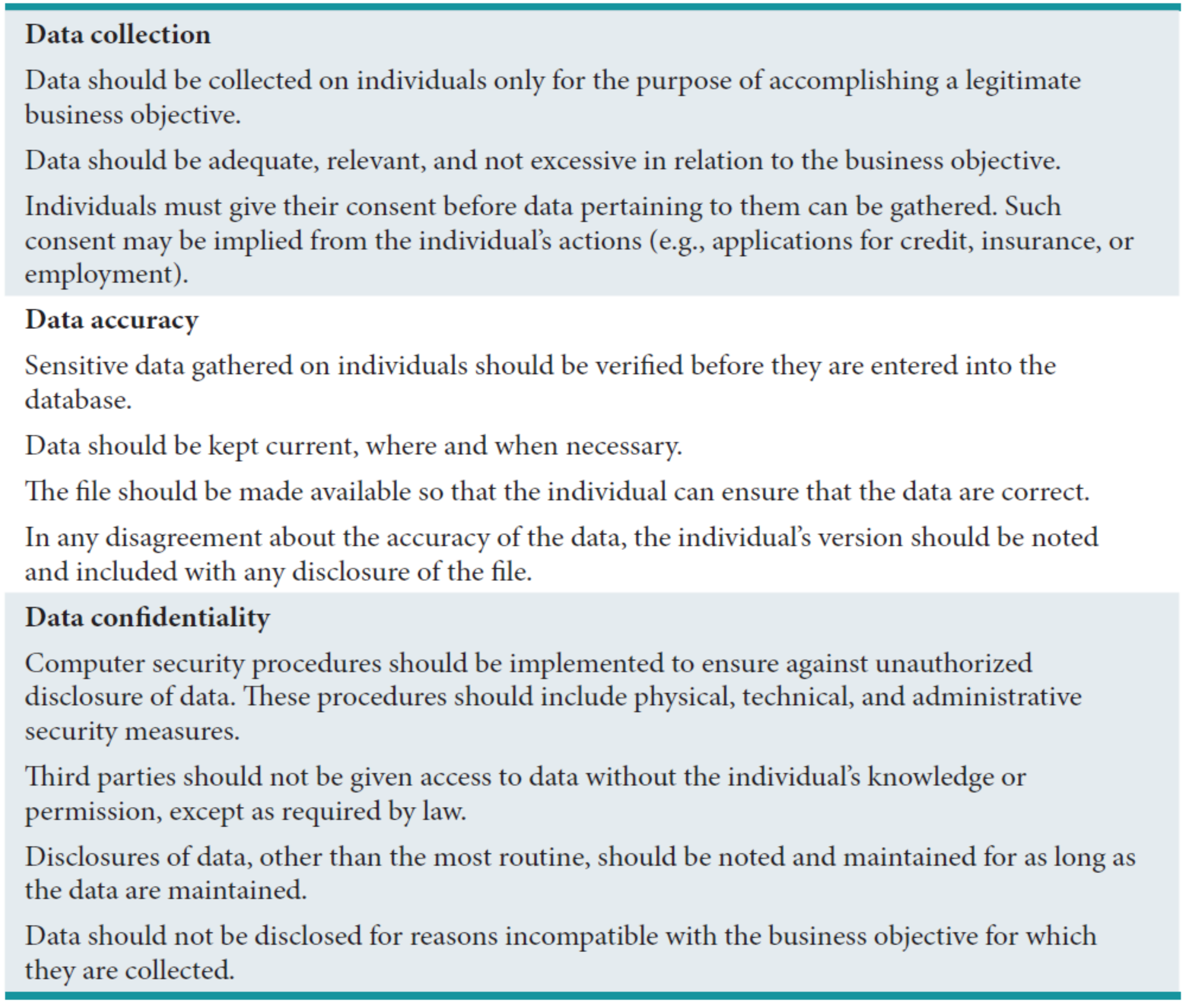
Privacy Codes and Policies

- Privacy policies or privacy codes are an organization’s guidelines for protecting the privacy of its customers, clients, and employees.
- Opt-in Model
- Opt-out Model
- Platform for Privacy Preferences (P3P)

Privacy Codes and Policies

- The **opt-out** model of informed consent permits the company to collect personal information until the customer specifically requests that the data not be collected.
- Privacy advocates prefer the **opt-in** model of informed consent, which prohibits an organization from collecting any personal information unless the customer specifically authorizes it

Privacy Policy Guidelines: A Sampler



Data collection

Data should be collected on individuals only for the purpose of accomplishing a legitimate business objective.

Data should be adequate, relevant, and not excessive in relation to the business objective.

Individuals must give their consent before data pertaining to them can be gathered. Such consent may be implied from the individual's actions (e.g., applications for credit, insurance, or employment).

Data accuracy

Sensitive data gathered on individuals should be verified before they are entered into the database.

Data should be kept current, where and when necessary.

The file should be made available so that the individual can ensure that the data are correct.

In any disagreement about the accuracy of the data, the individual's version should be noted and included with any disclosure of the file.

Data confidentiality

Computer security procedures should be implemented to ensure against unauthorized disclosure of data. These procedures should include physical, technical, and administrative security measures.

Third parties should not be given access to data without the individual's knowledge or permission, except as required by law.

Disclosures of data, other than the most routine, should be noted and maintained for as long as the data are maintained.

Data should not be disclosed for reasons incompatible with the business objective for which they are collected.