



Introduction to Information Systems

Data Science Education Program



Chapter #10

Ethics, privacy, and
security

Ethics, Privacy, and Security

LEARNING OBJECTIVES

- 1 Define ethics, describe two ethical frameworks, and explain the relationship between ethics and the law.
- 2 Explain how intellectual property and plagiarism pose challenges for information ethics, and describe technologies that are used to deal with them.
- 3 Describe information privacy and strategies to protect it, and explain why organizations may implement surveillance.
- 4 Explain the steps that organizations use to manage security risks, identify threats, assess vulnerabilities, and develop administrative and technical controls.
- 5 Explain why human behavior is often the weakest link for ethics, privacy, and security, and provide examples of strategies that can be used to counteract the weaknesses.

An online, interactive decision-making simulation that reinforces chapter contents and uses key terms in context can be found in [MyMISLab™](#).

INTRODUCTION

IN “VAMPIRE LEGENDS,” THE ONLINE DECISION-MAKING SIMULATION FOR THIS CHAPTER, you join a fiercely competitive company in the multiplayer game business. They are about to launch a sequel to their wildly successful first game, and the stakes are very high. They must roll it out on time, stay within budget, and do a brilliant marketing campaign. They also must be sure their IT infrastructure can handle whatever happens. With pressure so high, the team must make tough decisions as they confront choices dealing with ethics, privacy, and security.

This chapter and the simulation explore the responsibilities organizations and individuals share to treat data with care, make ethical decisions about its use, and protect it from countless threats. Game companies face intriguing problems in these areas, with the vast amount of private information they store and the endless hacking attempts. In addition, their customers are often very devoted to their online games and avatars.

Vampire Legends

A Role-Playing Simulation on Ethics, Privacy, and Security in the Multiplayer Online Game Business



Ethics, privacy, and security issues underscore how the human element is so tightly interwoven with the other three components of information systems: technology, processes, and data. People decide how to build

a system, manage it, secure it, and use the potentially priceless information it contains. Let's begin with ethics, and the kinds of ethical dilemmas people and organizations face in the digital world.

On-Line Simulation Exercise

- In this chapter and the online simulation called *Vampire Legends* you will:
 - Explore the responsibilities organisations and individuals share to treat data with care
 - Make ethical decisions about its use
 - Protect it from threats
- Game companies face intriguing problems in these areas, with the vast amount of private information they store and the endless hacking attempts.
- In addition, their customers are often very devoted to their online games and avatars

Key Terms and Concepts

KEY TERMS AND CONCEPTS

ethics
natural laws and rights
utilitarianism
intellectual property (IP)
digital rights management (DRM)

information privacy
proxy
information security
malware
botnets

distributed denial of service (DDoS)
phishing
risk matrix
incidence response plan
multifactor authentication

encryption
public key encryption
firewall
single sign-on
social engineering



Introduction

Introduction

- *Ethics*: we define ethics, describe two ethical frameworks, and explain the relationship between ethics and the law
- *Challenges*: we explain how intellectual property and plagiarism pose challenges for information ethics and describe technologies that are used to deal with them
- *Privacy*: we describe information privacy and strategies to protect it, and explain why organizations may implement surveillance.
- *Security*: we explain the steps that organizations use to manage security risks, identify threats, assess vulnerabilities, and develop administrative and technical controls
- *Human behaviour*: we explain why human behaviour is often the weakest link for ethics, privacy, and security, and provide examples of strategies

Overview

- Ethics, privacy, and security relate to:
 - Technology
 - Processes
 - Data
- People:
 - Design information systems
 - Build information systems
 - Manage information systems
 - Use the data and information in information systems
- Ethical dilemmas relate to both people and organizations



Ethics



Ethics Theory

Ethical Theory

- Ethics (or moral philosophy) is a branch of philosophy that involves concept of conduct and matters of value
- Ethics seeks to resolve questions of human morality by defining concepts such as:
 - Good and evil
 - Right and wrong
 - Virtue and vice
 - Justice and crime
- As a field of intellectual inquiry moral philosophy is related to the fields of
 - Moral psychology
 - Descriptive ethics
 - Value theory

Ethical Study

- There are 3 major areas of study within ethics:
 - *Meta-ethics*: address the theoretical meaning and reference of moral propositions and how their truth values (if any) can be determined
 - *Normative ethics*: address the practical means of determining a moral course of action
 - *Applied ethics*: address a person is *obligated* (or *permitted*) to do in a specific situation or a particular domain of action
- There are two types of person:
 - The *general* population
 - A *professional* individual

Ethical Theories

- Ethics is a difficult subject which is generally characterised by individual perceptions and fuzzy concepts
- There are two major ethical theories:
 - Kantian theory (Immanuel Kant – 1724-1804)
 - Essentially focused on the individual
 - Universal theory
 - Essentially focusses on a universal ethical principle
 - A concept in the universal theory is the maximum benefit for the majority
- The debate over ethical theory:
 - Has been around for millennia
 - It always has been, and remains, a very difficult topic

Ethical Frameworks

- Ethical frameworks
 - Natural laws and rights
 - Utilitarianism

FIGURE 10-1
Major ethical frameworks.

Ethical System	Description	Examples
Natural laws and rights	Actions are judged to be ethical or unethical according to how well they adhere to broadly accepted rules derived from natural law.	Thou shalt not kill. Right to privacy. Right to a free press. Liberté, égalité, fraternité.
Utilitarianism	Actions are ethical or unethical based on their consequences and outcomes.	The greatest good for the greatest number. The needs of the many outweigh the needs of the few.

Ethics

ethics

A system of moral principles that human beings use to judge right and wrong and to develop rules of conduct.

natural laws and rights

An ethical system that judges the morality of an action based on how well it adheres to broadly accepted rules, regardless of the action's actual consequences.

utilitarianism

An ethical system that judges whether an act is right or wrong by considering the consequences of the action, weighing its positive effects against its harmful ones.

Ethics, the Law and ICT

- Ethics and the law
 - Grounded in ethical principles
 - Law does not cover all ethical principles
 - Legality vs ethical principles
- Ethical issues and information and communications technologies (ICT)
 - ICT add important elements to ethical decision-making
 - IT affects decision-making in the on-line world
 - Freedom of speech
 - Ethical dilemmas
- **Figure 10.2.** is a short survey on ethical decisions

Figure 10.2.

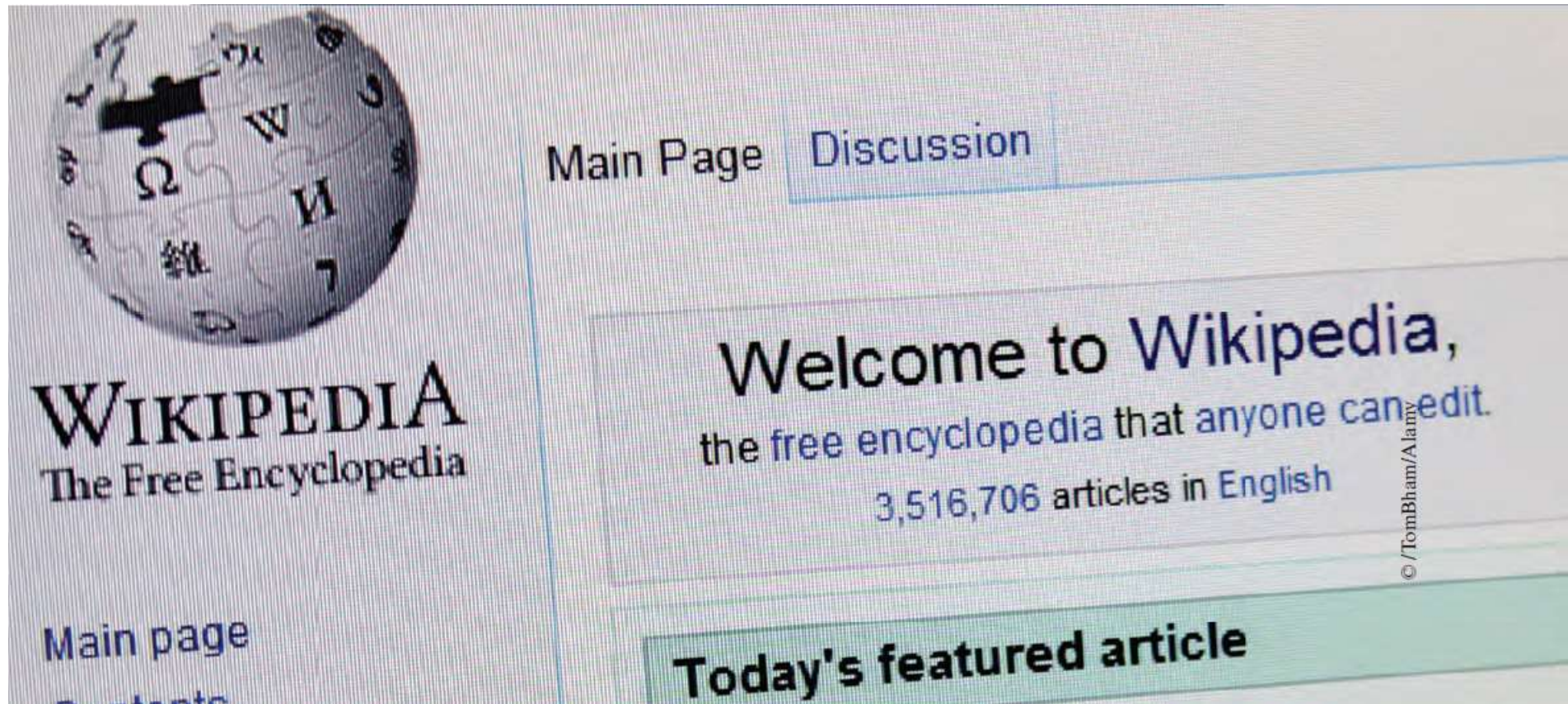
	Completely right, no punishment	1	2	3	4	5	6	Completely wrong, severe punishment
1. In a book store, accounting student K.F. slips an expensive CPA Exam Prep book into a shopping bag, then leaves the store without paying for the book.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. Marketing manager L.D. posts some negative reviews about a competitor on a review website, pretending to be various dissatisfied customers.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. Business student F.W., who asked to take the midterm early due to travel, meets several friends for coffee after the test, to tell them all the questions on it.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. Late for work, Assistant Manager J.T. cuts and pastes large segments from a website to finish a report on time, without citing the source.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. A sick friend asked M.B. for a special book on alternative medicines, so M.B. downloads a pirated copy without paying, and e-mails it to the friend.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6. Frustrated by incompetent managers who only promote their relatives, scientist R.P. secretly takes photos of the designs for the company's groundbreaking new medical device, then offers to bring them to the company's rival for a higher paying position there.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

FIGURE 10-2

Take this short survey on ethical decision making. Do you judge these actions as completely right, completely wrong, or somewhere in between?

Wikipedia

- Freedom of speech and ethical dilemmas





Information ethics

Information Ethics

- Intellectual property and digital management
 - Enforcement of intellectual property (IP) laws
 - Piracy
 - Protecting IP with technology and new business models
- Plagiarism
 - Intellectual property
 - Digital rights management
- Privacy
 - Privacy vs convenience (the 'trade-off')
 - Anonymity
 - Surveillance
 - The 'right to be forgotten'

Information Ethics: example dilemmas

Information Ethics Issue	Sample Dilemma
Intellectual property rights	Is it more important to protect intellectual property (IP) rights or to make information as widely available as possible? Will IP creators stop creating if there are fewer incentives?
Hacking	Is it ethical to break into the corporate network, not to do harm, but to demonstrate that the company needs better security?
Plagiarism	When a person gets an idea from reading another's work and then paraphrases it in a paper without crediting the source or even remembering where it came from, is that plagiarism? Or is it just forgetfulness?
Parasitic computing	Is it ethical to borrow a few CPU cycles from thousands of private computers without the owners' consent when they are not being used? What if the purpose is to do medical research?
Spam	Is it ethical to harvest millions of email addresses from websites and send them unsolicited commercial messages?

FIGURE 10-3
Information ethics issues and the dilemmas they present.

Intellectual Property

FIGURE 10-4

Survey of 15,000 computer users worldwide.

How often do you acquire pirated software or software that is not fully licensed?

Always	5%
Mostly	9%
Occasionally	17%
Rarely	26%
Never	38%
Don't know/refuse to answer	5%

Source: Business Software Alliance, (2012). Shadow Market: 2011 BSA Global Software Piracy Study, 9th edition, http://portal.bsa.org/globalpiracy2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf, accessed February 24, 2013.

intellectual property (IP)

Intangible assets such as music, written works, software, art, designs, movies, creative ideas, discoveries, inventions, and other expressions of the human mind that may be legally protected by means of copyrights or patents.

digital rights management (DRM)

Technologies that software developers, publishers, media companies, and other intellectual property owners use to control access to their digital content.

Software Licenses and Piracy

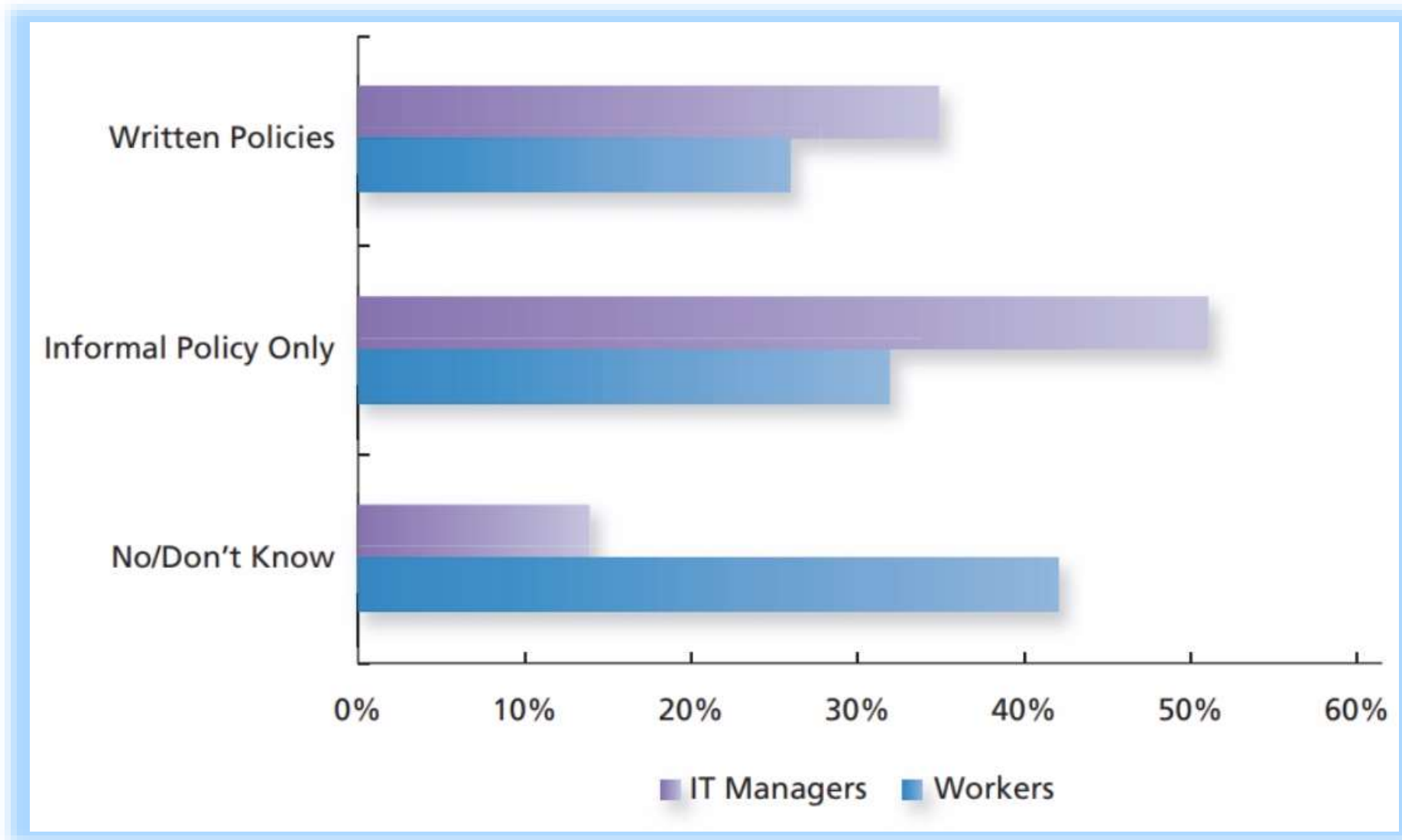


FIGURE 10-4

Does your company/organization have a policy about the use of unlicensed software?

Digital Rights Management

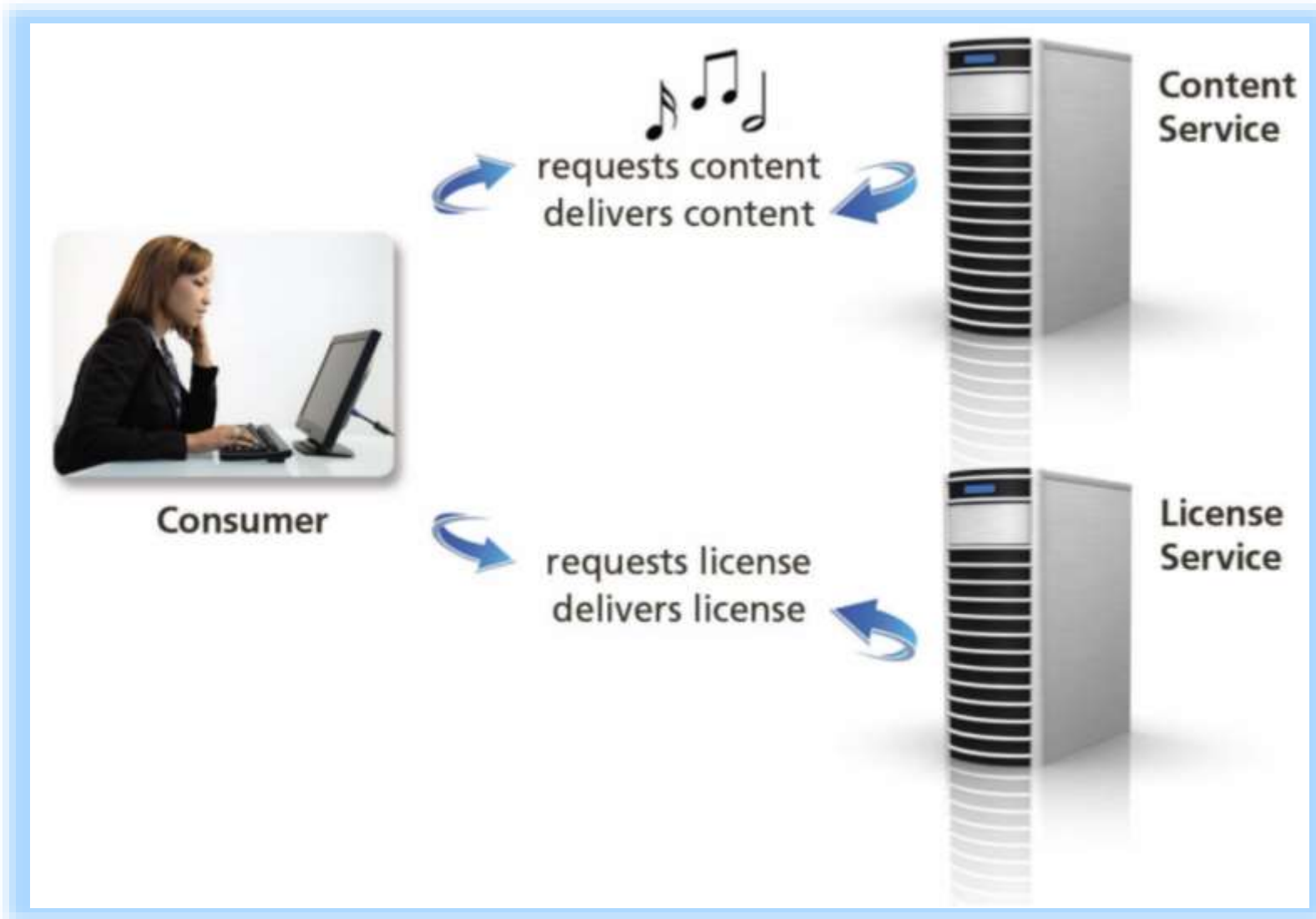


FIGURE 10-5

Digital rights management scheme.

DRM Records and Plagiarism

- When purchasing software or media:
 - Keep records of the purchase
 - This applies to both proprietary and FOSS software
 - Plagiarism is an infringement of intellectual property

PRODUCTIVITY TIP

When you purchase digital content, keep copies of online receipts, serial numbers, and confirmation numbers, just in case you have to contact customer support to reinstall it over DRM schemes.

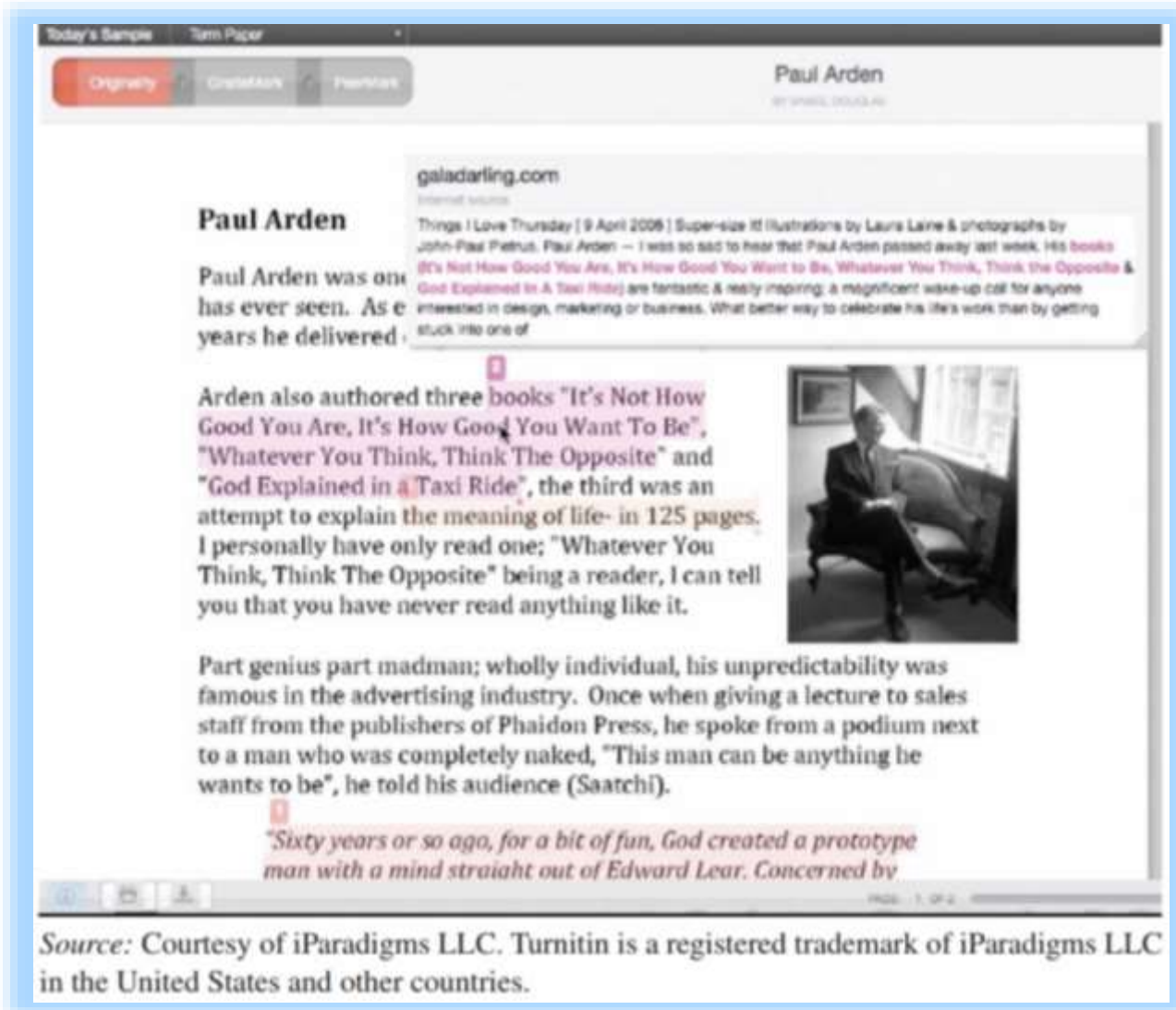
PRODUCTIVITY TIP

Students can use free originality-checking software, such as www.writecheck.com, to examine their own work for unintentional plagiarism. The output will show which sections are not original and will need citations.

Plagiarism

FIGURE 10-6

Checking written work for originality and possible plagiarism.





Privacy

Privacy

- What is privacy and why is it important?
 - Privacy is elusive – an issue with developments in technology
 - Information privacy
- Important factors to consider:
 - Trading privacy for convenience and freebies
 - Anonymity
 - Surveillance
 - The right to be forgotten

information privacy

The protection of data about individuals.

proxy

An intermediary server that receives and analyzes requests from clients and then directs them to their destinations; sometimes used to protect privacy.

Figure 10.7. and Privacy

FIGURE 10-7
Elements of privacy.

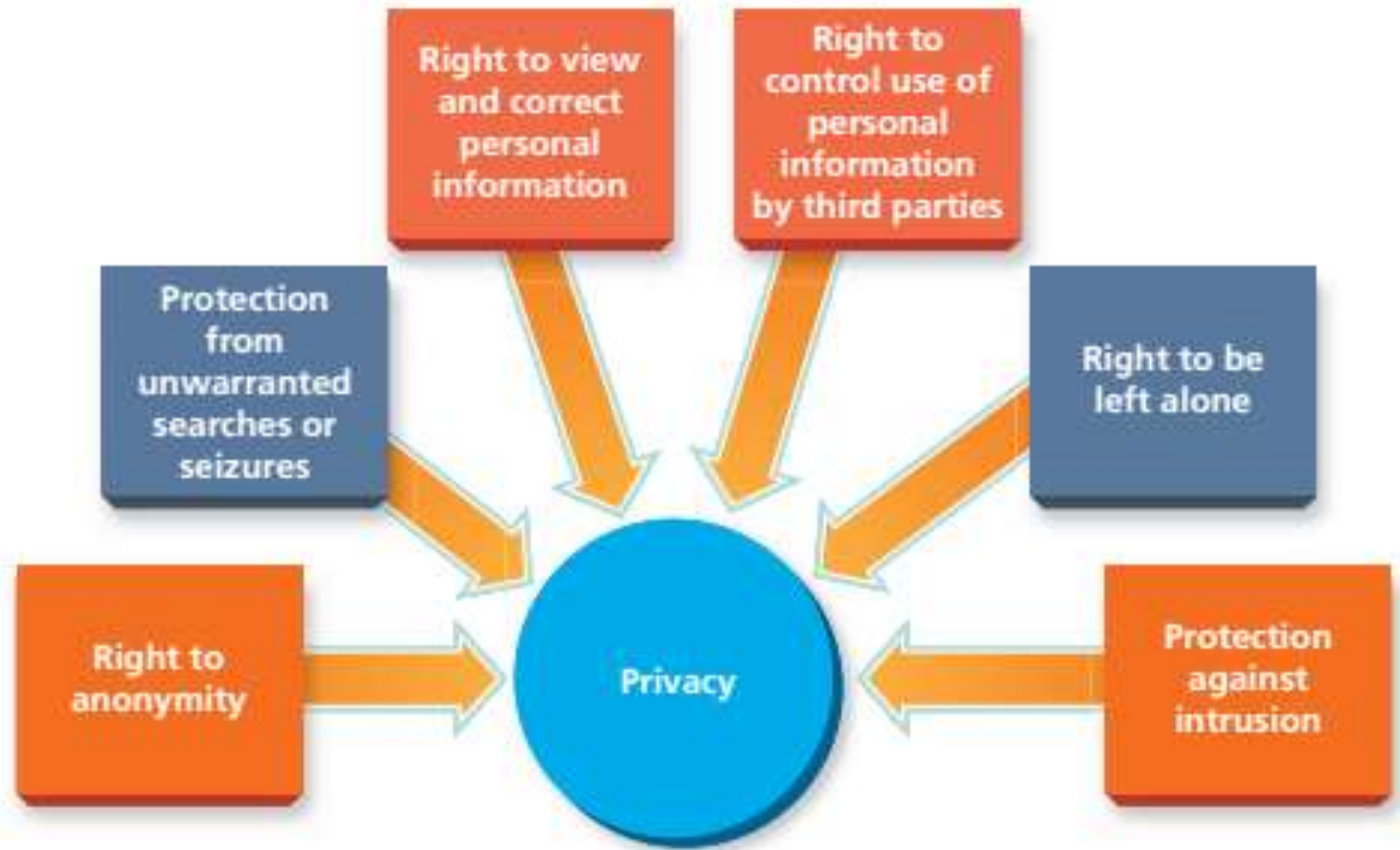


Figure 10.8. and Anonymity



FIGURE 10-8

Proxy servers can be used to mask a web surfer's IP address.

Anonymity and Distributed Servers



FIGURE 10-9

A network of distributed servers can relay a transmission and hide its source.

Surveillance

- Surveys show that employers lean toward surveillance for several reasons:
 - Concerns about employer liability for allowing harassment or hostile work environments
 - Need to protect security and confidentiality
 - Concerns about employee productivity and “cyberslacking”
 - Concerns about bogging down corporate servers with personal files

The Right to be Forgotten

Tips for Reducing Digital Footprints

- ▶ Check your privacy settings on all of your social networking sites.
- ▶ Remove accounts that you no longer use.
- ▶ Before you post something online, think about whether you'd mind if it appeared in a national newspaper, with your name attached.
- ▶ If your posts include information about other people, think about whether they would mind if that information appeared in a national newspaper.
- ▶ Try using the Tor browser.
- ▶ Wipe clean all information on digital devices before you recycle them.

FIGURE 10-10

Tips for reducing digital footprints.

What happens to a person's digital assets when he or she dies? Do the heirs inherit all the iTunes songs and Kindle e-books? What about all the photos and videos on social networking sites, or the level 99 warrior in an online game? While a few states have passed laws attempting to clarify these issues, companies like Google and Facebook are fighting them. The issue remains muddled, and will have to be tested in the courts.¹⁴



Information security

Information Security

- Risk management
- Identifying threats
 - Malware and botnets
 - Distributed denial of service (DDoS)
 - Phishing and vishing
 - Information leakage
- Assessing vulnerabilities
- Administrative security controls

information security

A term that encompasses the protection of an organization's information assets against misuse, disclosure, unauthorized access, or destruction.

PRODUCTIVITY TIP

Before entering sensitive data into any form on a website, check for the <https://> in the address bar to be sure transmissions are encrypted. Click on the padlock symbol to see security details.

PRODUCTIVITY TIP

The administrative controls you establish for your own computer will help protect your information assets. Turning off the computer at night, for instance, will reduce your exposure to intrusion attempts, and save energy, too.

Information Security

- Technical security controls
 - Authentication strategies
 - Encryption
 - Intrusion prevention and detection systems
 - Firewalls
 - Blocking spam
- Information security and cloud computing
 - Security considerations
 - Standards and best practices

Cloud Computing and Information Security

- Information security and cloud computing
 - Security considerations
 - Standards and best practices
- Types of clouds?
 - Public cloud
 - Private cloud
 - Hybrid cloud
- Software-as-a-service (SaaS)
- Legal and contractual control of data and services

Information Asset Protection

- **Figure 10.10.** identifies:
 - Issues risk managers must be aware of and manage

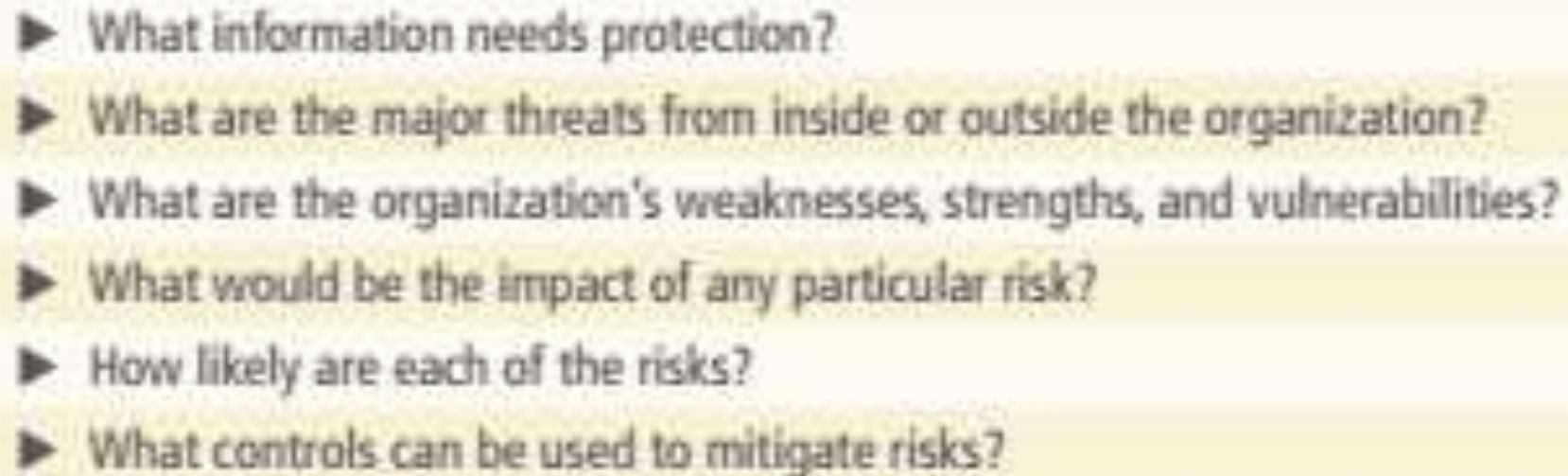
- 
- ▶ What information needs protection?
 - ▶ What are the major threats from inside or outside the organization?
 - ▶ What are the organization's weaknesses, strengths, and vulnerabilities?
 - ▶ What would be the impact of any particular risk?
 - ▶ How likely are each of the risks?
 - ▶ What controls can be used to mitigate risks?

FIGURE 10-10
Issues for risk managers.

Identifying Threats

- Threats may come from many sources and include:
- Identifying threats
 - Malware and botnets
 - Distributed denial of service (DDoS)
 - Phishing and vishing
 - Information leakage

Threats to Information Security

FIGURE 10-11

Types of information security threats.

Human Threats

Accidental misuse, loss, or destruction by employees, consultants, vendors, or suppliers

Actions by disgruntled employees, insider theft, sabotage, terrorism, hackers, spam

Environmental Threats

Fire
Floods
Earthquakes
Hurricanes
Industrial accidents
War
Power failures
Arson



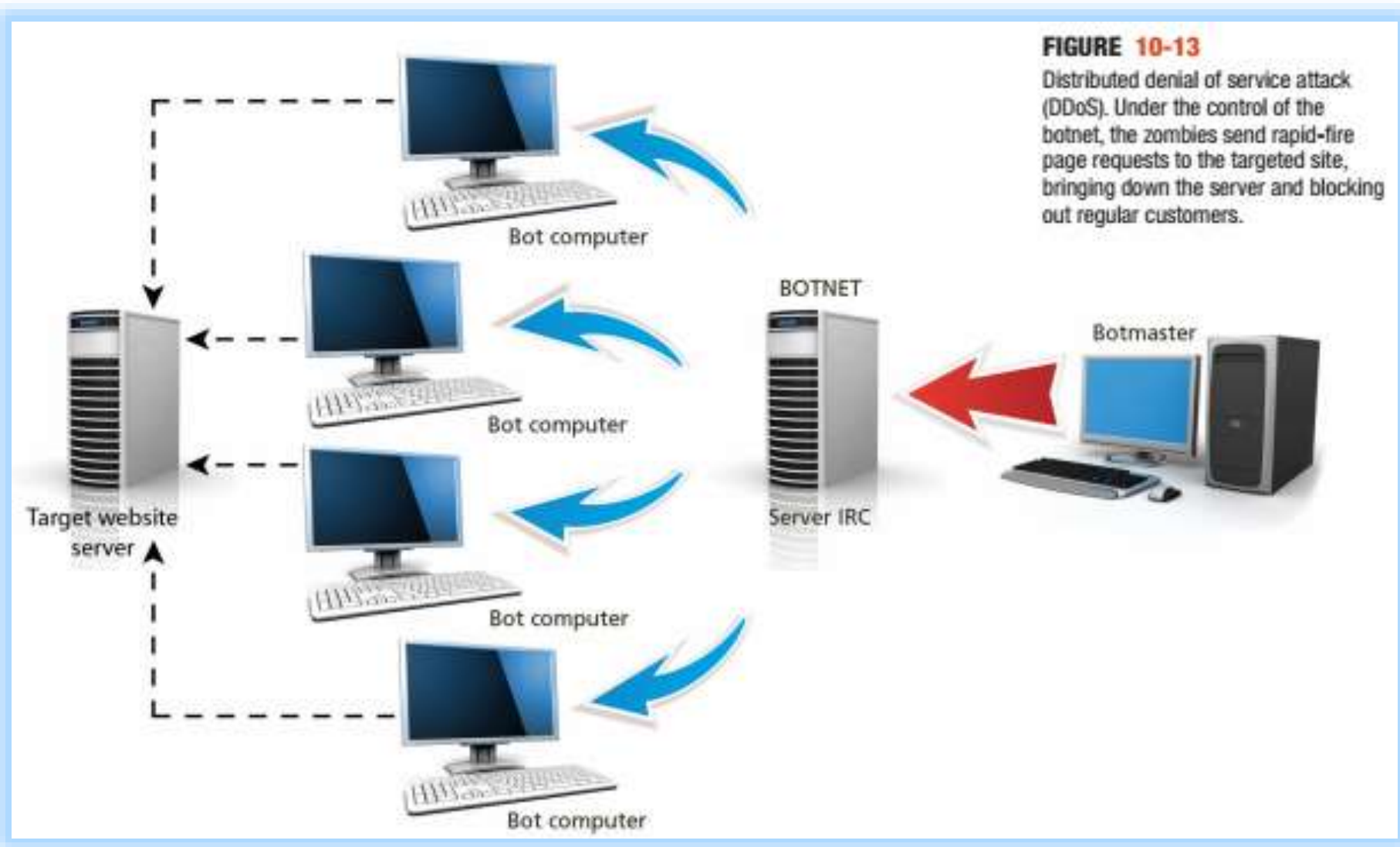
Examples of Malware

FIGURE 10-12

Examples of malware.

Malware	Description
Computer virus	A malicious software program that can damage files or other programs. The virus can also reproduce itself and spread to other computers by email, instant messaging, file transfer, or other means.
Spyware	Software that monitors a user's activity on the computer and on the Internet, often installed without the user's knowledge. Spyware may use the Internet connection to send the data it collects to third parties.
Keylogger	Monitoring software that records a user's keystrokes.
Worm	A self-replicating program that sends copies to other nodes on a computer network and may contain malicious code intended to cause damage.
Trojan horse	A seemingly useful, or at least harmless, program that installs malicious code to allow remote access to the computer, as for a botnet.

DDoS Attacks



Ethical Considerations and DDoS Attacks



THE ETHICAL FACTOR

Ethical Dilemmas in a Distributed Denial of Service Attack

Scenario: An elementary school librarian is trying to install some software to create avatars from students' photos so they won't be tempted to upload their own photos. She fails the first time, but rather than phone the vendor, the librarian tries turning off the firewall and antivirus software. That works, and the librarian turns the security back on.

Two weeks later, the school's whole network goes down. The school's IT technician can see that the server's CPU is overloaded with Internet traffic, but can't do anything. By noon, the harried principal is wondering whether to close the school since so much depends on computers, from bus scheduling and reporting to communications and academic records. At 1:30, the principal receives a call from the security officer of a government agency in Canada, who says the school's server was turned into a zombie by a botnet and used in a denial of service attack against the agency. The agency's minister insisted on stopping the attack at once, so the officer triggered a counterattack to target the zombies as quickly as possible. First embarrassed,

then angry, the principal says, "But this is an elementary school! You can't just bring it down like that without telling us. It's not ethical. What if this were a hospital?!" The principal ponders suing someone, but isn't sure who to blame. The officer complains that no one can identify who created the botnet, or who paid to use it to launch this DDoS.

The well-intentioned librarian took a shortcut to install software and made the school's network vulnerable. Once the malware was installed and the DDoS against the government agency got underway, the security company in Canada used intrusion-detection techniques to identify the zombies by their IP addresses. That company was tasked with stopping the DDoS, so its staff quickly shut down the zombies with a counterattack, without taking time to learn who they were or what impact that decision might have. Recovering from this event will cost the school considerable time and money.

The scenario involves many players: the librarian, the principal, the school's IT technician, the security officer in Canada, the agency's minister, the botnet creator, and the one who purchased use of the botnet and set off the DDoS. How would you evaluate their ethical decision making?

A Typical Phishing Email

FIGURE 10-14

Sample phishing email.

From: Internal Revenue Service [mailto:admin@irs.gov]
Sent: Wednesday, March 01, 2006 12:45 PM
To: john.doe@jdoe.com
Subject: IRS Notification - Please Read This



After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of \$63.80. Please submit the tax refund request and allow us 6-9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please [click here](#)

Regards,
Internal Revenue Service

© Copyright 2006, Internal Revenue Service U.S.A. All rights reserved.

Source: www.irs.gov/pub/irs-utl/phishing-email.pdf.

malware

Malicious software designed to attack computer systems.

botnet

A combination of the terms *robot* and *network* referring to a collection of computers that have been compromised by malware and used to attack other computers.

distributed denial of service (DDoS)

An attack in which computers in a botnet are directed to flood a single website server with rapid-fire page requests, causing it to slow down or crash.

phishing

An attempt to steal passwords or other sensitive information by persuading the victim, often in an email, to enter the information into a fraudulent website that masquerades as the authentic version.

Information Leakage Events

FIGURE 10-15

Sample information leakage events.

Organization and Date	Event
Facebook.com, June 21, 2013	Facebook discovered a bug that allowed unauthorized users to view personal contact information of other users.
Goldman Sachs, Bloomberg, May 18, 2013	Reporters for Bloomberg News could tap into Bloomberg's data terminals to monitor client's activities.
NBC.com, February 22, 2013	NBC's website was hacked to steal passwords and usernames.
Express Scripts, Ernst & Young, February 18, 2013	A partner snuck into the headquarters and apparently emailed over 20,000 pages of data to himself.
Haagen-Daz, February 14, 2013	Thieves connected a flash drive with key-logging software to a cash register to collect customers' credit card information.

Source: Chronology of data breaches—Security breaches 2005–Present. Privacy Rights Clearinghouse. www.privacyrights.org/data-breach, accessed September 23, 2013.

Information Leakage Events

Organization and Date	Event
Internal Revenue Service February 10, 2016	Automated cyberattack on the e-filing system, leaking e-file PINs
Snapchat March 4, 2016	Successful phishing scam targeting the company's payroll department
BeautifulPeople.com, April 26, 2016	Hackers gained personal information on 1.1 million users of the online dating site
Office of Personnel Management, June 4, 2015	21.5 million government personnel records hacked, exposing employees' personnel data
<i>Source:</i> Based on Chronology of data breaches—Security breaches 2005–Present. Privacy Rights Clearinghouse. http://www.privacyrights.org/ , accessed October 7, 2016.	

Assessing Vulnerability

- Vulnerability assessment may employ a number of techniques including:
 - Risk assessment and controls
 - Risk matrix (see Figure 10.16. which shows a simplified risk matrix)

risk matrix

A matrix that lists an organization's vulnerabilities, with ratings that assess each one in terms of likelihood and impact on business operations, reputation, and other areas.

Vulnerability	Leak of Confidential Data	Lost Integrity, Reputation	Systems Unavailable	Financial Risk	Likelihood That Event Will Happen	Total Impact Rating
No backup power for a workstation	1	2	8	2	4	4
Loss of unencrypted backup data	10	10	4	7	3	6.8

FIGURE 10-16
Simplified risk matrix.

Administrative Security Controls

- Figure 10.17. shows:
 - The steps to be implemented in an incident response plan
 - The five steps are:
 1. Identify the threat
 2. Contain the damage
 3. Determine the cause
 4. Recover the systems
 5. Evaluate the lessons learned
 - Note:
 - Step four will require data back-up and disaster recovery planning

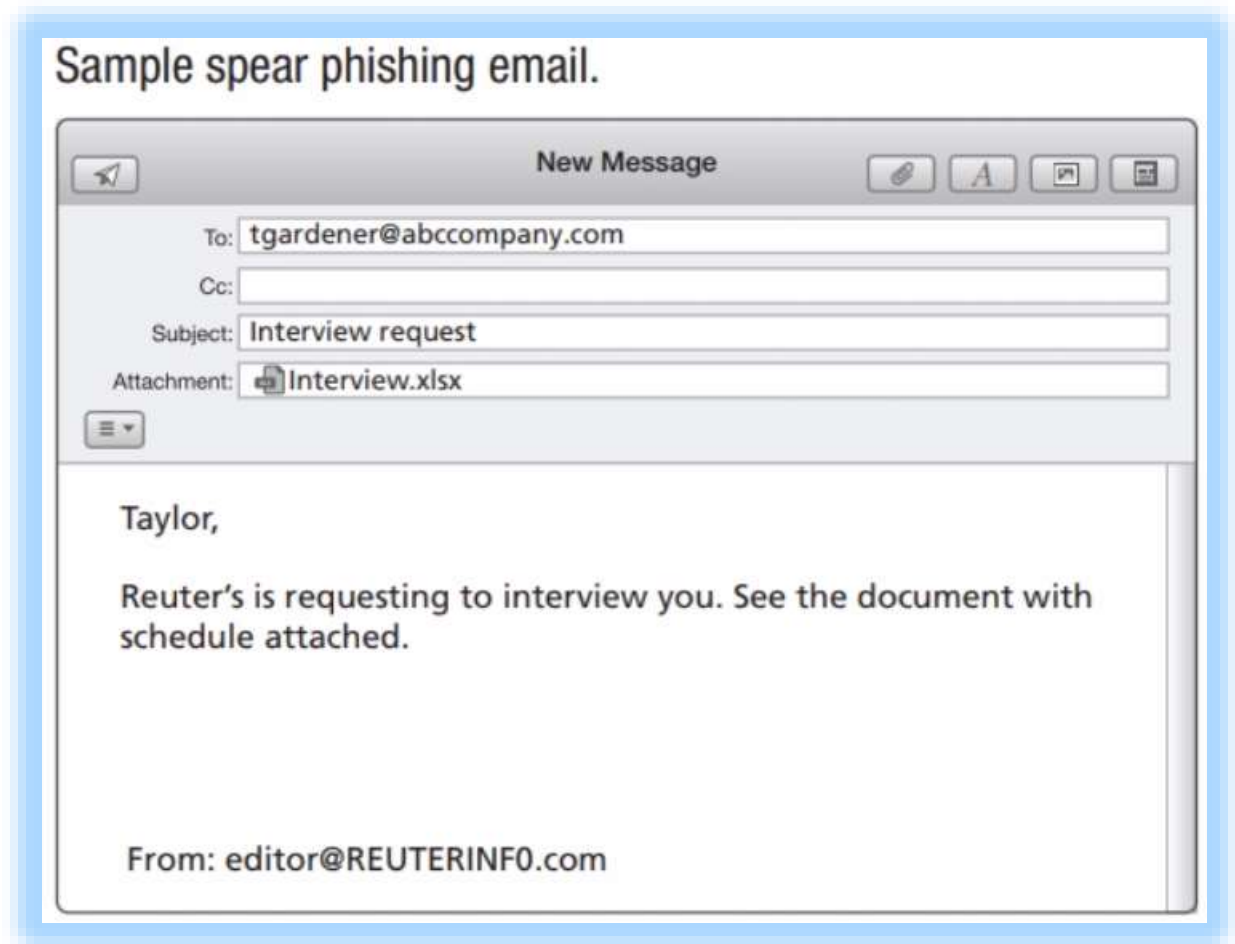
FIGURE 10-17

Steps in an incident response plan.



Example of a Spear Phishing Email

- Phishing can take a number of forms:
 - *Phishing*: an email distributed at random with no specific target
 - *Spear phishing*: where the target is identified with some personal information
- There is also *vishing*:
 - This takes the form of a voice call over a telephone



Administrative Security Controls

FIGURE 10-18

Examples of administrative and technical controls.

Category	Administrative Control Examples	Technical Control Examples
Account management	The organization requires appropriate approvals for requests to establish accounts.	The information system automatically disables accounts after a time period defined by the organization.
	The organization monitors for atypical usage of information system accounts.	The information system automatically logs any account creations, modifications, or termination actions.
Access controls	The organization defines the information to be encrypted or stored offline in a secure location.	The information system enforces approved authorizations for access to the system.
	The organization defines the privileged commands for which dual authorization is to be enforced.	The information system prevents access to any security-relevant information contained within the system.
Information flow	The organization defines the security policy that determines what events require human review.	The information system enforces the organization's policy about human review.
Separation of duties	The organization separates duties of individuals as necessary to prevent malevolent activity without collusion.	The information system enforces separation of duties through access control.

Blocking Spam

- Preventing (or at least mitigating) spam:
 - Authentication strategies
 - Encryption
 - Intrusion prevention
- Methods used include the creation of a:
 - White list
 - Black list
 - User generated rules
 - Intelligent (rule-based) systems to spot spam

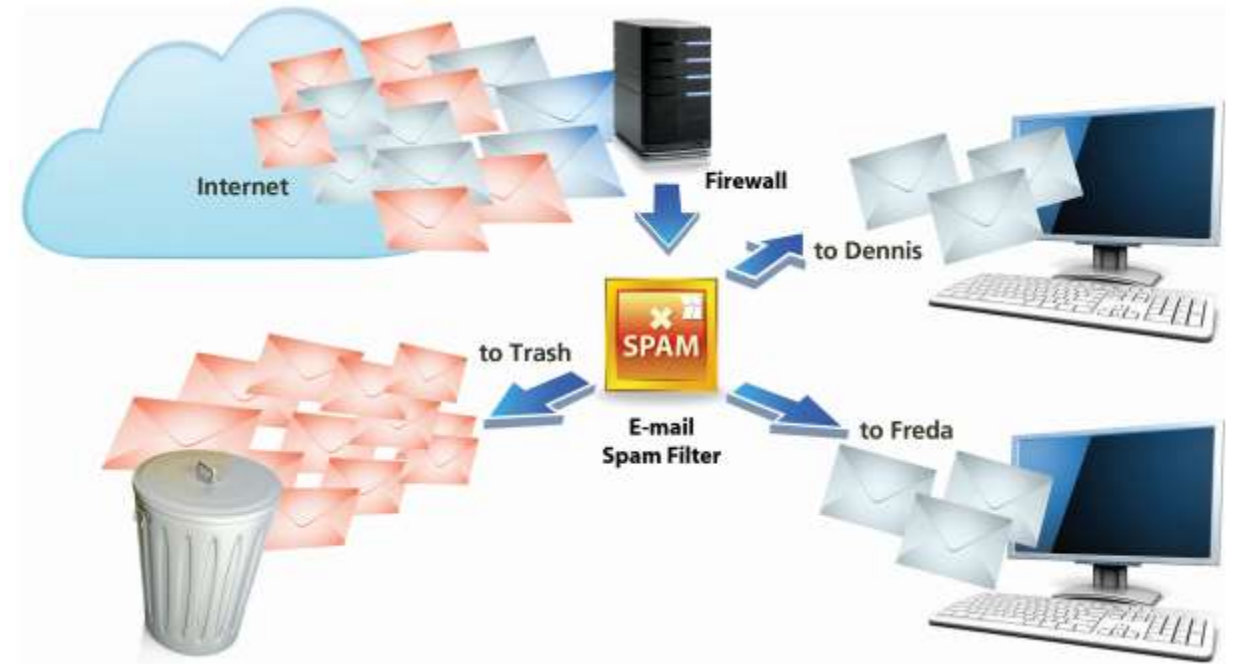


FIGURE 10-19
Blocking spam.

Information Security

- Information security is important for many reasons including:
 - The demands of legal, regulatory, and compliance
 - Trust and reputational factors
 - Financial considerations

incidence response plan

A plan that an organization uses to categorize a security threat, determine the cause, preserve any evidence, and also get the systems back online so the organization can resume business.

multifactor authentication


A combination of two or more authentications a user must pass to access an information system, such as a fingerprint scan combined with a password.

encryption

Technique that scrambles data using mathematical formulas, so that it cannot be read without applying the key to decrypt it.

public key encryption

A security measure that uses a pair of keys, one to encrypt the data and the other to decrypt it. One key is public, widely shared with everyone, but the other is private, known only to the recipient.



The human element in
information ethics,
security, and privacy

Ethics and Information Systems

- Human behavior and decision making play a central role in almost any situation combining information ethics, privacy, and security
- Indeed, human beings are very often the weakest link for a number of reasons
- In considering *social engineering and information security* we must address a broad range of factors including:
 - Human traits
 - Respect for authority
 - Humans and greed
 - Scammers
 - Avoidance of malware
 - Scareware and email scams

Security Awareness

- Organizations must implement robust security programs
- Security programs must address:
 - Corporate policies
 - Legal, statutory, and compliance regulations
 - Processes to manage security compliance
 - Networking
 - Cloud-based systems policies

Compliance Requirements

FIGURE 10-23

Examples of laws touching on information security and privacy.

Law/Regulation	Description
Privacy Act of 1974	Establishes requirements that govern how personally identifiable information on individuals is collected, used, and disseminated by federal agencies.
Health Insurance Portability and Accountability Act (HIPAA)	Includes provisions to protect the privacy and security of individually identifiable health information.
Family Educational Rights and Privacy Act (FERPA)	Establishes privacy rights over educational records. For example, federally funded educational institutions must provide students with access to their own educational records and some control over their disclosure.
CAN-SPAM Act	Prohibits businesses from sending misleading or deceptive commercial emails, but denies recipients any legal recourse on their own. The act also requires companies to maintain a do-not-spam list.
Gramm-Leach-Bliley Act	Stipulates how financial institutions are required to protect the privacy of consumers' personal financial information and notify them of their privacy policies annually.
Driver's Privacy Protection Act of 1994	Limits the disclosure of personally identifiable information that is maintained by state departments of motor vehicles.
State Security Breach Notification Laws	Require organizations to notify state residents if sensitive data are released. The wording varies by state.
European Union's Data Protection Directive	Establishes privacy as a fundamental human right for EU citizens. The law is more restrictive than U.S. laws. For example, it requires companies to provide "opt out" choices before transferring personal data to third parties.

Security Awareness

- Weak passwords
- Reducing complexity
- Social engineering
- Security awareness

- ▶ Do not include personal information such as names, addresses, or phone numbers.
- ▶ Avoid real words.
- ▶ Mix different character types, including lowercase, uppercase, and special characters.
- ▶ To reduce the cognitive load of memorizing the password, create "pass phrases" with meaningful chunks and use the first letter of each word, such as "I love whitewater rafting_Done it 15 times" (llwwr_Di15t).
- ▶ Use different passwords for each login you want to secure, so loss of one does not compromise the others.
- ▶ Change your passwords every 30 to 60 days, or as required by the application.

FIGURE 10-22
Creating secure passwords.

Security Awareness

PRODUCTIVITY TIP

Your college or university probably has spam blocks in place, but no filter is perfect. Check your junk mail occasionally in case messages you want to receive were trapped by the filter. Identify any false positives as “not junk” so the sender’s messages are not trapped again.

firewall

A defensive technical control that inspects incoming and outgoing traffic and either blocks or permits it according to rules the organization establishes. The firewall can be a hardware device or a software program.

Passwords

- **Figure 10.20.** shows suggestions to create secure passwords including:
 - Avoid weak passwords
 - Be security aware

FIGURE 10-20

Creating secure passwords.

- ▶ Do not include personal information such as names, addresses, or phone numbers.
- ▶ Avoid real words.
- ▶ Mix different character types, including lowercase, uppercase, and special characters.
- ▶ To reduce the cognitive load of memorizing the password, create "pass phrases" with meaningful chunks and use the first letter of each word, such as "I love whitewater rafting_Done it 15 times" (Ilwvr_Di15t).
- ▶ Use different passwords for each login you want to secure, so loss of one does not compromise the others.
- ▶ Change your passwords every 30 to 60 days, or as required by the application.

Reducing Password Complexity

- To reduce the complexity and cognitive load associated with multiple passwords:
 - Organizations implement the single sign-on with a single user ID and password
 - This provides a gateway service to multiple software applications
- Complexity can also affect privacy decisions:
 - Few people ever read the T&C (while the T&C often contain conditions that impact privacy)
- Social networking sites:
 - Balance users' privacy concerns against their own need to generate advertising revenue through targeted marketing that relies on information about each user's preferences and friendship network
 - Facebook is often at the center of privacy debates:
 - Not just for its own policies but for the terms users agree to when they play social games
 - The case study at the end of this text explores how Facebook confronts privacy issues

Social Engineering and Security

FIGURE 10-21

Social engineering: Would you hold the door for these people so they don't have to search for their ID badges?



FIGURE 10-22

Scareware persuades people that a computer is infected when it is not. The solution the victim pays for may be harmless or it may install its own malware.



Security Awareness and Ethical Decision-Making (1)

- Consider the extent of harm each of these actions might inflict on other people
 - A sales rep copies customer data to her smartphone and quickly drops it into a jacket pocket. Corporate policy forbids taking confidential documents out of the building, but she just wants to work on them at home to catch up. She leaves her jacket on the subway but says nothing to her supervisor about the incident
 - A sixth grader finds a USB drive in a school computer and sees the names and addresses of all the students and teachers. He uploads it to his social networking account so all his friends have contact information

Security Awareness and Ethical Decision-Making (2)

- A university employee looks up old academic records of political candidates and sends some provocative tit-bits to the press
- A co-worker suspects an employee of accessing illicit websites at work but hesitates to mention it because it might get the employee in big trouble or even fired
- The CFO asks someone in IT to delete his whole email account from the server and backup media because it contains messages that suggest criminal behaviour
- How would you judge the actions of these people?

Security Awareness and Ethical Decision-Making (3)

- These cases show how closely tied ethics, privacy, and security are, and how humans make decisions about small and large issues almost daily and:
 - Sometimes the decisions are easy to make
 - However: often they present dilemmas that challenge even people who understand security and who try hard to make ethical decisions
- As information systems grow even more powerful and interconnected:
 - Protection of valuable informational assets will be increasingly important and urgent



Summary

Review

- In this session we have considered:
 - Ethics, ethical frameworks, and the relationship between ethics and the law
 - Challenges including intellectual property, plagiarism for information ethics, and technologies used to deal with them
 - Privacy including strategies to protect it and why organizations implement surveillance.
 - Security and the steps that organizations use to manage security risks, identify threats, assess vulnerabilities, and develop administrative and technical controls
 - Human behaviour with consideration of why human behaviour is often the weakest link for ethics, privacy, and security, and provide examples of strategies

On-Line Simulation Exercise

MyMISLab | Online Simulation

Vampire Legends

A Role-Playing Simulation on Ethics, Privacy, and Security in the Multiplayer Online Game Business



The massively multiplayer online game business is lucrative, but very competitive. Your company has poured millions into the game, adding vivid graphics, tense storylines,

and many features to support collaboration and team play, and the strategy is paying off. You are very proud of the way you were able to use social media to spread the word and persuade people to try it out. Most noticed right away that the avatars move very smoothly and they are much easier to configure and control compared to other games. That's thanks to the terrific IT staff, who also made programming breakthroughs so players could do more quests from their smartphones. A number of celebrities even play the game, although under false names and in disguise.

Now that the game's sequel is ready to release, you and the other senior execs must work out the strategy and budget. Everyone thinks Ancient Age of Vampires will be even more successful than the original game, and analysts project a significant revenue increase. Log in when you're ready to get to work. . . .

LEARNING OBJECTIVES

- 1** Ethics is a system of moral principles used to judge right from wrong. One ethical framework focuses on natural laws and rights. A second, called utilitarianism, emphasizes the consequences of actions. Although many laws are grounded in ethical principles, actions can be legal but not ethical or ethical but not legal. Most people tend to judge unethical behavior, such as plagiarism or intellectual property theft, less harshly when the violator uses a computer and the Internet compared to similar acts committed in face-to-face settings.
- 2** Information ethics focuses on the storage and transmission of digitized data and raises both ethical and legal issues. Although most countries protect intellectual property (IP), digitized IP is extremely difficult to protect, and many companies use digital rights management technologies to safeguard their assets. Plagiarism has also become very difficult to prevent because of ICT, although it can also be much more easily detected with originality-checking tools.
- 3** Privacy is under considerable pressure because of the growing volume of personal information online, the complexity of privacy settings and privacy policies, and users' willingness to trade privacy for convenience. Services that use proxies can offer anonymity for online activity. Surveillance poses threats to privacy, but employers often choose to implement surveillance because of concerns about liability, security, confidentiality, and productivity. Some governments are debating whether to pass laws that give people the "right to be forgotten" with respect to information that companies collect about them online.
- 4** Information security ensures the protection of an organization's information assets against misuse, disclosure, unauthorized access, or destruction. Organizations use risk management to identify assets needing protection, identify the threats, assess vulnerabilities, and determine the impact of each risk. Threats arise from both human and environmental sources and include accidental events, intentional attacks from insiders or external criminals, fires, floods, power failures, and many more. Distributed denial of service and phishing attacks are common threats that result in significant downtime and leakage of sensitive information. Administrative controls encompass the policies, procedures, and plans the organization creates and enforces to protect information assets and respond to incidents when they occur. Technical controls are implemented by the information systems and include strategies such as encryption and user authentication. Intrusion prevention and detection systems block traffic and activity based on the rules the organization develops and alert managers if suspicious activity occurs. The firewall is an important element for intrusion prevention. Standards for information security for cloud computing are under development but are critical to the future of this architectural trend.
- 5** Human beings prize productivity highly and may neglect security when it interferes. Social engineering tactics take advantage of human behavioral tendencies to manipulate people into disclosing sensitive information or bypassing security measures. Training in security awareness and the relationships between security, ethics, and privacy can help counteract these tendencies.

KEY TERMS AND CONCEPTS

ethics	information privacy	distributed denial of service (DDoS)	encryption
natural laws and rights	proxy	phishing	public key encryption
utilitarianism	information security	risk matrix	firewall
intellectual property (IP)	malware	incidence response plan	single sign-on
digital rights management (DRM)	botnets	multifactor authentication	social engineering

CHAPTER REVIEW QUESTIONS

- 10-1.** What are ethics? What are two broad categories of ethics? What approach does each category take? What are examples of each category of ethics? What is the difference between ethics and the law?
- 10-2.** What is intellectual property (IP)? What are the information ethics associated with IP? What is the impact of digital media on the information ethics of IP? What are examples of technologies used to control access to digitized intellectual property?
- 10-3.** What is plagiarism? What are the information ethics associated with plagiarism? What is the impact of digital media on the information ethics of plagiarism? What are examples of technologies used to detect plagiarism?
- 10-4.** How do social media sites help users in protecting their privacy?
- 10-5.** Why do organizations implement surveillance? What are the advantages of surveillance? What are the disadvantages of surveillance?
- 10-6.** What are the steps that organizations take in order to manage information security risks and build a risk matrix? What is involved in each step of this process?
- 10-7.** Which information security threats are people exposed to when they surf the Internet and download content from it?
- 10-8.** What are information security vulnerabilities? How do organizations assess vulnerability?
- 10-9.** What are the steps involved in the development of an incident response plan?
- 10-10.** What are examples of technical controls that organizations implement to improve security?
- 10-11.** Why is human behavior often the weakest link for information ethics, information privacy, and information security? What are examples of strategies that organizations can implement to counteract the weaknesses in human behavior and decision making that have a negative impact on information security and privacy?

PROJECTS AND DISCUSSION QUESTIONS

- 10-12.** According to Wikipedia.org, digital rights management is used by organizations such as Sony, Amazon, Apple, Microsoft, AOL, and the BBC. What is digital rights management? Why do organizations use technology to protect intellectual capital? Describe a typical DRM application that can be used to manage access to digital content. Are there disadvantages to using DRM?
- 10-13.** Two dreaded "P" words for college students are *procrastination* and *plagiarism*. Does the first action necessarily lead to the second? Visit Plagiarism.org to learn more about the various forms of plagiarism. How are the different types of plagiarism similar? How are they different? What are the consequences of plagiarism at your university? Consult your student handbook to learn how plagiarism is defined by your school and how faculty members may respond to cases of plagiarism. What are the options for discipline in cases of plagiarism? Prepare a 5-minute presentation of your findings.
- 10-14.** The Identity Theft Resource Center® is a nonprofit organization dedicated to helping users understand and prevent identity theft. Visit Google.com and search for "ITRC Fact Sheet 101" or visit www.idtheftcenter.org and select "Consumer Resources" and "ID Theft Test" to locate "ITRC Fact Sheet 101: Are You at Risk for Identity Theft." Answer 20 self-test questions relating to document disposal, Social Security number protection, information handling, and scams to determine your ID theft risk score. Are you savvy about identity theft risks or do you need to take some corrective actions? Prepare a 5-minute presentation to share with your classmates.
- 10-15.** Do you trade privacy for convenience? Visit Google.com and select "About Google" to locate the "Privacy & Terms" link located at the bottom of the page. Follow this link to "Policies and Principles," then locate the "Privacy Policy" link at the bottom of this page. Does Google place cookies on your computer or other devices? Why do they use cookies? What are location-enabled services? Does Google have information about your actual location? Under what circumstances does Google share personal information with other companies? How do you describe the information security measures that Google takes to safeguard access to personal information? Is there anything in the privacy policy that makes you uncomfortable? Are you likely to change your Google search habits as a result of reviewing its privacy policy?
- 10-16.** Malware is malicious software that is developed for the purpose of causing harm. What are different types of malware? How does malware infiltrate a computer system? What is a botnet? Why do criminals use botnets? What is a distributed denial of service attack? What are three ways that DDoS attacks impact organizations? Visit Microsoft.com and search for "malicious software removal tool." How frequently does Microsoft release a new version of this tool? Search Microsoft.com to learn more about how to boost your malware defense and protect your PC. Prepare a brief summary of your findings.
- 10-17.** Why is it important to verify the identity of computer users? What are three authentication strategies? Which is the strongest form of authentication? Which is the weakest? What credentials does your university use to

Zynga Kills Petville and Angers Virtual Pet Owners

Social game developer Zynga is a leading player in the industry, with 240 million active users in more than 175 countries. It features popular titles such as Castleville, Mafia Wars, Farmville 2, Words with Friends, and Zynga Poker. Most people play the games with their friends on Facebook or on Zynga's own site (Zynga.com). Founded by Mark Pincus in 2009, Zynga's popularity exploded in 2012, when revenue topped \$1.2 billion. Expenses for game development and acquisitions are high, however, so despite 12.8% sales growth, the company posted a loss in net income.

Unlike most online game companies, Zynga earns over 90% of its revenue from in-game purchases of virtual goods rather than advertising. The games are free to play, but advancement can take a long time. Players who want to advance more quickly can use their PayPal accounts to purchase game currency, energy points, or virtual goods.

Social games rise and fall in popularity, and Zynga pulls the plug on games that falter. One of the games the company killed off with barely two weeks' notice was Petville, and outraged players were furious. Many had invested years in nurturing and caring for their digital pets, sharing the adventure with their friends and family on Facebook. Thousands posted their sadness and anger on social media sites, with comments like those in Figure 10-25.

Clearly, the players had an emotional investment in their virtual pets, and also in the social dimension of the game that Zynga's software specifically encourages. For example, players earned points by visiting neighbors, who were actually real-life friends with their own virtual pet in the game. Points mounted up quickly as more neighbors joined and exchanged gifts.

Zynga tracks and analyzes player behavior closely, and uses the "big data" to add features that ensure players log in frequently to

develop that strong attachment. Zynga wisely chose not to let someone's virtual pet die from hunger if the player did not feed it daily. However, the pet was taken to the pound, and the owner had to find ways to earn enough cash to retrieve it.

Zynga offered credits for its other games, but Petville players were quite dismayed by the company's lack of sensitivity. Certainly, companies have to shut down badly performing products, but there is a difference between terminating a line of shampoo and killing off a game like Petville. Customers are not likely to mourn the loss of a favorite hair product in the same way they would a virtual puppy they have been nurturing for years.

Even though the terms of service agreement gave the company vast leeway to terminate services or close down games, and Zynga's metric-driven business strategy justified the shut-down, its approach generated a lot of ill will. At best, it was a customer relations blunder, but it also raised ethical questions. The company's software is specifically designed to create such emotional ties, so observers thought that the company should have recognized they existed and arranged for a more sensitive closing. Certainly more advance notice was warranted. Rather than assume players would happily switch to another game and forget about their pets, Zynga might have held online ceremonies to bid farewell, or planned a clever happy ending in which the pets founded their own world together.

Zynga is no longer closely tied to Facebook, which was taking a cut of Zynga's profits. Its own website, Zynga.com, is open to anyone who loves gaming, whether a Facebook user or not. The company's future is unclear, and time will tell whether Zynga can use its big data to better understand its own customers and develop a profitable business.

FIGURE 10-25

Comments from players who objected to Zynga's decision to shut down Petville.

- ▶ "I loved my bunny now I will never get to see her again—it is not fair at all."
- ▶ "My autistic son and I had played Petville together for two years...I wish you 'people' could have seen the streams of tears running down both our faces as we played our last session. We even took photographs. I guess money trumps everything!"
- ▶ "This is the last day my little friend will be alive. So sad."
- ▶ "My daughter is heartbroken."
- ▶ "Zynga [stinks]!! And I will NEVER play any of your games again. You can take your lousy credits and shove them! I hope Karma comes around to get you and you think back on how many people you upset and lost due to [the] stupid, greedy decision to remove Petville."

verify your identity for access to email and other web-based information such as personal financial aid information and online course materials? Is this strong or weak authentication? What is a security token? Visit Wikipedia.org to learn how security tokens are used to authenticate users and prepare a brief report of your findings. Do you think it is a good idea to use security tokens to authenticate students? Why or why not?

- 10-18. Did you ever wonder why junk email is called "spam"? The Monty Python sketch on spam has been viewed over five million times on YouTube. That's a lot of spam! Work in a small group with classmates to consider why spam is one of the biggest problems facing the Internet today. Approximately how much email traffic is made up of spam? Is spam a problem on mobile devices? Why is spam a problem for consumers? Why is it a problem for organizations

and Internet service providers? What types of technical controls do organizations use to combat spam? Prepare a brief report of your group discussion.

- 10-19. Recall from Chapter 3 how cloud computing generally requires leasing IT resources, depending on a third party to store data or provide services. Work in a small group with classmates to consider the security risks associated with cloud computing. Why are IT managers concerned about protecting cloud-based information assets? What is the IT industry response to concerns about cloud computing? What is the Cloud Security Alliance? Consider the class registration application at your university. Does your group consider this a mission-critical application? Why or why not? Prepare a 5-minute presentation of your discussion that includes a recommendation for or against using cloud computing for critical applications at your university.

APPLICATION EXERCISES

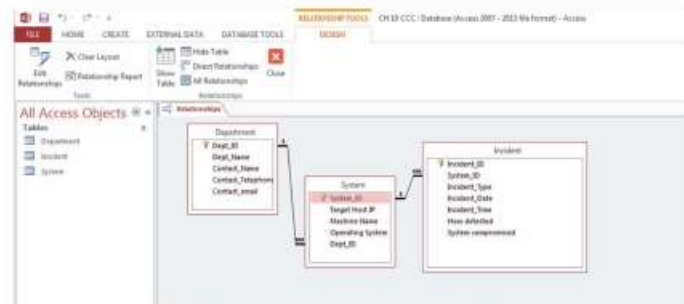
10-20. EXCEL APPLICATION:
Citywide Community College

The IT Department at Citywide Community College developed a computer security incident response plan that requires users to provide information for each security incident. Louis Hermann, the IT manager, inventoried the major components of the college's computer systems and created a spreadsheet to track the equipment by manufacturer, model number, and serial number. He decided to confine the list to major computer components, and he does not try to track keyboards, mice, and so forth. Louis then created a spreadsheet to track systems security incident facts including information about the department reporting the incident, target-specific information (host machine name, etc.), source-specific information (source IP address), and information about the type of security incident or attack. Louis has asked you to use the data provided in the CCC Security spreadsheet, Ch10Ex01, to identify (1) the department reporting the highest number of security incidents and (2) the most prevalent type of intrusion. Use the "countif" function to count the number of security incidents in which

the computer system was compromised. Use a memo format to submit a summary of your findings to Louis.

10-21. ACCESS APPLICATION:
Citywide Community College

Louis Hermann, IT manager at Citywide Community College, is working with two spreadsheets to manage computer security incident reporting. One spreadsheet tracks the major components of the college's computer systems, and the other spreadsheet tracks security incident facts. To provide for better reporting capabilities, Louis wants you to set up an Access database that tracks college departments, computer systems, and security incidents. Download the spreadsheet Ch10Ex02 and import the worksheets to create the database shown in Figure 10-24. Create a report that lists the number of security incidents reported by each department. Create a second report that lists the number of attacks in which the system was compromised for the department having the greatest number of security incidents. What other reports would Louis find useful?

FIGURE 10-24
Citywide Community College security database.

Discussion Questions

- 10-22.** When Zynga dropped Petville abruptly, virtual pet owners protested that they had been harmed. This ethical argument uses a utilitarian framework. How might you argue from a natural laws and rights ethical framework that Zynga was wrong?
- 10-23.** The suddenness of Zynga's action created a firestorm of customer discontent. What are other ways that Zynga might have handled the discontinuance of a failing game without creating such protest?
- 10-24.** Can the reaction of Petville customers pose a risk to Zynga's future?

- 10-25.** When virtual pet owners invested emotionally and financially in "their" pets, should they have been considered at least partial owners of the digital information? Why or why not?

Sources: Farewell to Fido: A lesson in digital customer relationship management. (January 30, 2013). Knowledge @ Wharton, <http://knowledge.wharton.upenn.edu/article.cfm?articleid=3178>, accessed March 30, 2013.
Huston, C. (2013). Zynga, Inc. Hoover's Online, <http://subscriber.hoovers.com/proxy3.library.jhu.edu/11company360/overview.html?companyId=16184800000000>, accessed July 8, 2013.
Rosenbush, S., & Totty, M. (March 11, 2013). How big data is changing the whole equation for business. The Wall Street Journal, <http://search.proquest.com/docview/1315526655?accountid=11752>, accessed July 8, 2013.

CASE STUDY #2

Community Policing on the Internet: Spamhaus Targets Worldwide Spammers and Draws a Massive Distributed Denial of Service Attack

Silently protecting the inboxes of billions of people worldwide is an international nonprofit organization called Spamhaus, which describes its four-point mission as:

- ▶ Tracking the Internet's spam operations.
- ▶ Providing dependable real-time anti-spam protection for Internet networks.
- ▶ Working with law enforcement agencies to identify and pursue spammers worldwide.
- ▶ Lobbying governments for effective anti-spam legislation.

With headquarters in the United Kingdom and Switzerland, Spamhaus maintains a "block list" containing the IP addresses believed to originate spam. Many governments, corporations, universities, and other organizations check the list before delivering mail, blocking any messages whose senders match an entry on it.

Identifying and Fighting Spammers

How do senders wind up labeled as spammers and placed on the block list? Spamhaus defines spam as any mail that is both unsolicited and sent in bulk. Mail that meets this definition may not be illegal in many places, including the United States, so Spamhaus is the target of lawsuits claiming damages for lost business. For example, a Chicago email marketing firm called "e360" sued Spamhaus for more than \$11 million in damages. A U.S. court eventually awarded e360 \$27,000, but Spamhaus refuses to pay even that amount, insisting that e360 is a spammer. Although e360 is now out of business, its main employee complains bitterly about this kind of community policing that works outside of traditional law enforcement. "Spamhaus.org is a fanatical, vigilante organization that operates in the United States with blatant disregard for U.S. law," he said.

Although the cause is noble, the stakes are extremely high, so the work itself can be both dangerous and secretive. Larry, Spamhaus's

chief technical officer, who prefers not to reveal his last name, says, "We get threats every day. In the U.S., it is people bringing lawsuits against us. And then there are organized criminals in Russia and Ukraine, who use different methods." Police have advised Steve Linford, head of Spamhaus, to be suspicious of any unexpected packages delivered to his home.

Spamhaus Hit with DDoS Attack

In March 2013, a massive distributed denial of service (DDoS) attack, one of the largest in Internet history, hit the Spamhaus website. The attackers used "DNS reflection," in which the Internet's domain name servers, which resolve URLs to their corresponding IP addresses, are spoofed into sending huge traffic streams to one website. Spamhaus crashed, and the enormous attack left many wondering if the whole Internet might be in danger.

Sven Kamphuis quickly took credit for the attack, accusing Spamhaus of trying to "control the Internet through underhanded extortion tactics." Kamphuis heads a company named CyberBunker; this company offers a hosting service that does not keep any traffic logs, so there are no records for police to confiscate. Spammers and copyright violators flock to hosts like this, and Spamhaus had blocked several of CyberBunker's clients, some of whom volunteered to launch the DDoS attack. Police arrested Kamphuis in Spain a few weeks afterwards.

Pros and Cons of Community Policing

Industry analysts know that community policing is not perfect and that block lists can contain false positives that harm legitimate businesses. It is time-consuming and expensive for companies to work through the process to get cleared. But as one analyst put it, "These [spammers] aren't just a nuisance. They're a cancer on society. And Linford has taken it upon himself to do something about them. . . . That these cops are self-appointed is troubling. But marketers would do well to understand that without Spamhaus, people's inboxes would be unusable."

Discussion Questions

- 10-26.** How do the interests of computer users differ from the interests of spammers?
- 10-27.** Do you agree with the Spamhaus methodology to reduce spam?
- 10-28.** What other approaches could be taken to reduce spam?
- 10-29.** Is it ethical for Spamhaus to label senders like e360 as spammers, considering that it can ruin their business?

Sources: Anderson, N. (June 16, 2010). Accused spammer demands \$135M from Spamhaus; gets \$27,002. Ars Technica, <http://arstechnica.com/tech-policy/news/2010/06/accused-spammer-demands-135m-from-spamhaus-gets-27002.ars>, accessed June 4, 2011.
Constantin, L. (2013). DDoS attack against Spamhaus was reportedly the largest in history. CIO, (13284045), 7.

Kirk, J. (2013). Spamhaus warns marketers to keep email databases tidy. CIO, (13284045), 39.
Palmer, M. (2009). Secret war on web crooks revealed. Financial Times (London). June 15, p. 16.
Riley, M., Matlack, C., & Levine, R. (2013). CyberBunk: Hacking as performance art. Bloomberg Businessweek, (4324), 33–34.
Tam, D. (March 27, 2013). Did the spam cyber fight really slow down the Internet? CNET News, http://news.cnet.com/8301-1009_3-57576699-83/did-the-spam-cyber-fight-really-slow-down-the-internet/, accessed April 25, 2013.
Tam, D. (April 26, 2013). Police arrest Dutchman for alleged Spamhaus web attacks. CNET News, http://news.cnet.com/8301-1009_3-57581639-83/police-arrest-dutchman-for-alleged-spamhaus-web-attacks/, accessed April 25, 2013.
Vijayan, J. (2013). Spamhaus attacks expose huge open DNS server dangers. CIO, (13284045), 35.

E-PROJECT 1 Tracking the Trackers: Investigating How Third-Party Cookies Steer the Ads You See

This e-project will show how third-party cookies read by a browser can shape the user's online browsing experience across websites.

First, you will need to remove existing cookies so you can conduct the experiment with a clean slate. Once they have been removed, configure your browser to accept new third-party cookies. (Check your browser's "help" if you need assistance.)

Next, visit online retailer Zappos (zappos.com) and look around for a product you would never actually purchase. Examine the product, clicking on features, and then add it to your cart. The goal is to add the third-party cookies about your visit and your shopping interests. Don't buy anything, of course. Zappos participates in quite a few ad networks, and each one will place a cookie on your computer.

- 10-30. Browse to several sites that carry advertising, such as yahoo.com, latimes.com, time.com, aol.com, and bloomberg.com. Search each page to see if there are any Zappos ads. Which websites show an ad from Zappos? Which ones did not show any Zappos ads? What was the content of the ads?

- 10-31. Remove all your cookies again, and revisit the same list of sites. What Zappos ads do you see now?

- 10-32. Explain the results that you found in this e-project. (Don't forget to reconfigure your browser to the privacy settings you prefer.)

E-PROJECT 2 Analyzing Spammers by Country, Using Excel Pivot Tables

In this e-project, you will explore Spamhaus's Registry of Known Spam Operators (ROKSO), a list the organization maintains and posts on its website.

Visit www.spamhaus.org and click on ROKSO. How does Spamhaus determine who or what should be in the registry?

Download the file Ch10_SpamHaus, which contains a list of known spammers from 2011.

- 10-33. Sort the list by the TopTen column. Which entry is considered the #1 spammer?

- 10-34. Next, you will generate a pivot table and chart showing the list of countries, with the count of each country's known spammers. Select the data in all columns and then choose Insert,

Pivot Chart. Drag and drop Country to the Axis Fields, and Name to the Values box, so the chart shows the count of spammers by country.

- Which country has the most known spammers?
- Which country is second in terms of the number of known spammers on this list?

- 10-35. To view a chart containing just the Top Ten offenders by country, click on IsOnTopTen in the Field List, and then click the down arrow to the right. Uncheck "no" so the analysis will only include spammers who are on the top 10 list. Drag the IsOnTopTen field to the Report Filter box. Which countries have the most spammers in the top ten?



Excel Exercise

Chapter #10 Practical Exercise

- In this lectures this week we have introduced:
 - Chapter #10
- Complete the following practical exercise:
 - Chapter #9: Excel Application 10.20. (Citywide Community College)
 - Access the Excel file *Ch10Ex01* (see Moodle)
 - You have been asked you to use the data provided in the CCC Security spreadsheet (Ch10Ex01) to identify:
 1. The department reporting the highest number of security incidents
 2. The most prevalent type of intrusion.
 3. Use the *countif* function to count the number of security incidents in which the computer system was compromised.
 4. Use a memo format to submit a summary of your findings to the systems administrator (Louis).