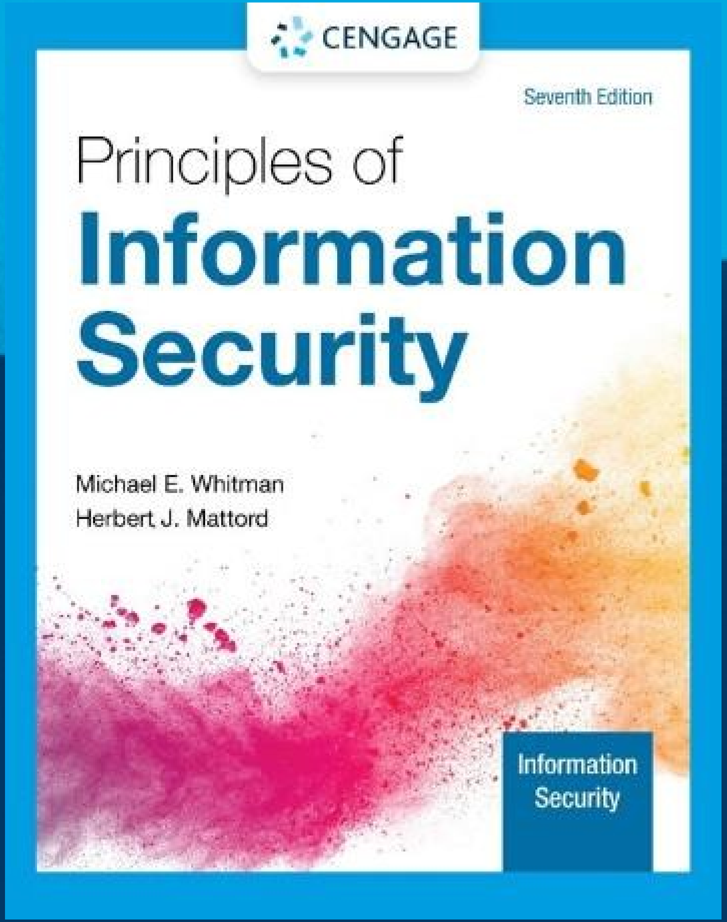


Module 6

Legal, Ethical, and Professional Issues in Information Security

CENGAGE

Module Objectives

Upon completion of this material, you should be able to do the following:

6.1 Explain the differences between laws and ethics.

6.2 Describe the relevant laws, regulations, and professional organizations of importance to information security.

6.3 Identify major national and international laws that affect the practice of information security.

6.4 Discuss the role of privacy as it applies to law and ethics in information security.

6.5 Explain the roles of some U.S. national law enforcement agencies with an interest in information security.

Introduction to Law and Ethics in Information Security

- As a future InfoSec professional, you must understand the scope of an organization’s legal and ethical responsibilities.
- To minimize liabilities and reduce risks, the information security practitioner must be able to do the following:
    - Understand the current legal environment.
    - Stay current with laws and regulations.
    - Watch for new and emerging issues.

Law and Ethics in Information Security

- Laws: rules that mandate or prohibit certain behavior and are enforced by the state.
- Ethics: regulate and define socially acceptable behavior.
- Cultural mores: fixed moral attitudes or customs of a particular group.
- Laws carry the authority of a governing authority; ethics do not.
- Liability: the legal obligation of an entity extending beyond criminal or contract law; includes the legal obligation to make restitution.
- Restitution: the legal obligation to compensate an injured party for wrongs committed.

Organizational Liability and the Need for Counsel

- Jurisdiction: court’s right to hear a case if the wrong was committed in its territory or involved its citizenry.
- Long-arm jurisdiction: application of laws to those residing outside a court’s normal jurisdiction; usually granted when a person acts illegally within the jurisdiction and leaves.
- Due care: the legal standard requiring a prudent organization to act legally and ethically and know the consequences of actions.
- Due diligence: the legal standard requiring a prudent organization to maintain the standard of due care and ensure actions are effective.

Policy Versus Law (1 of 2)

- Policies are managerial directives that specify acceptable and unacceptable employee behavior in the workplace.
- Policies function as organizational laws and must be crafted and implemented with care to ensure they are complete, appropriate, and fairly applied to everyone.
- Difference between policy and law: Ignorance of a policy is an acceptable defense ignorance of law is not.

Policy Versus Law (2 of 2)

- Criteria for policy enforcement:
  - Dissemination (distribution)
  - Review (reading)
  - Comprehension (understanding)
  - Compliance (agreement)
  - Uniform enforcement

Knowledge Check Activity 1

Business policies function as ______ laws and must be crafted and implemented with care to ensure they are complete, appropriate, and fairly applied to everyone.

a. national

b. state

c. organizational

d. city

Knowledge Check Activity 1: Answer

Business policies function as _____ laws and must be crafted and implemented with care to ensure they are complete, appropriate, and fairly applied to everyone.

Answer: c. organizational

Explanation.

Business polices are not directly aligned with criminal or civil laws although they must be aligned with them. Policies are the rules inside the business.

Types of Law

- Constitutional
- Statutory
  - Civil
    - Tort
  - Criminal
- Regulatory or Administrative
- Common, Case and Precedent
- Private vs Public

Relevant U.S. Laws

- The United States has been a leader in the development and implementation of information security legislation.
- Information security legislation contributes to a more reliable business environment and a stable economy.
- The United States has demonstrated understanding of the importance of securing information and has specified penalties for individuals and organizations that breach civil and criminal law.

General Computer Crime Laws (1 of 3)

- Computer Fraud and Abuse Act of 1986 (CFA Act): Cornerstone of many computer-related federal laws and enforcement efforts.
- National Information Infrastructure Protection Act of 1996:
  - Modified several sections of the previous act and increased the penalties for selected crimes.
  - Severity of the penalties was judged on the value of the information and the purpose, for example:
    - For purposes of commercial advantage.
    - For private financial gain.
    - In furtherance of a criminal act.

General Computer Crime Laws (2 of 3)

- USA PATRIOT Act of 2001 provides law enforcement agencies with broader latitude in order to combat terrorism-related activities.
- USA PATRIOT Improvement and Reauthorization Act made permanent fourteen of the sixteen expanded powers of the Department of Homeland Security and the FBI in investigating terrorist activity.
- USA FREEDOM Act inherited select USA PATRIOT functions as the PATRIOT act expired in 2015.
- Computer Security Act of 1987 is one of the first attempts to protect federal computer systems by establishing minimum acceptable security practices.

General Computer Crime Laws (3 of 3)

- FISMA: In 2002, Congress passed the Federal Information Security Management Act (FISMA), which mandates that all federal agencies establish information security programs to protect their information assets.
- FISMA was updated by the Federal Information Security Modernization Act of 2014 (a.k.a. FISMA Reform), which specifically focused on enhancing the federal government’s ability to respond to security attacks on government agencies and departments.

Privacy (1 of 2)

- Privacy has become one of the hottest topics in information security.
- It is the right of individuals or groups to protect themselves and their information from unauthorized access, providing confidentiality.
- The ability to develop information aggregation from multiple sources allows creation of information databases previously impossible.
- The number of statutes addressing an individual’s right to privacy has grown dramatically.

Information Aggregation

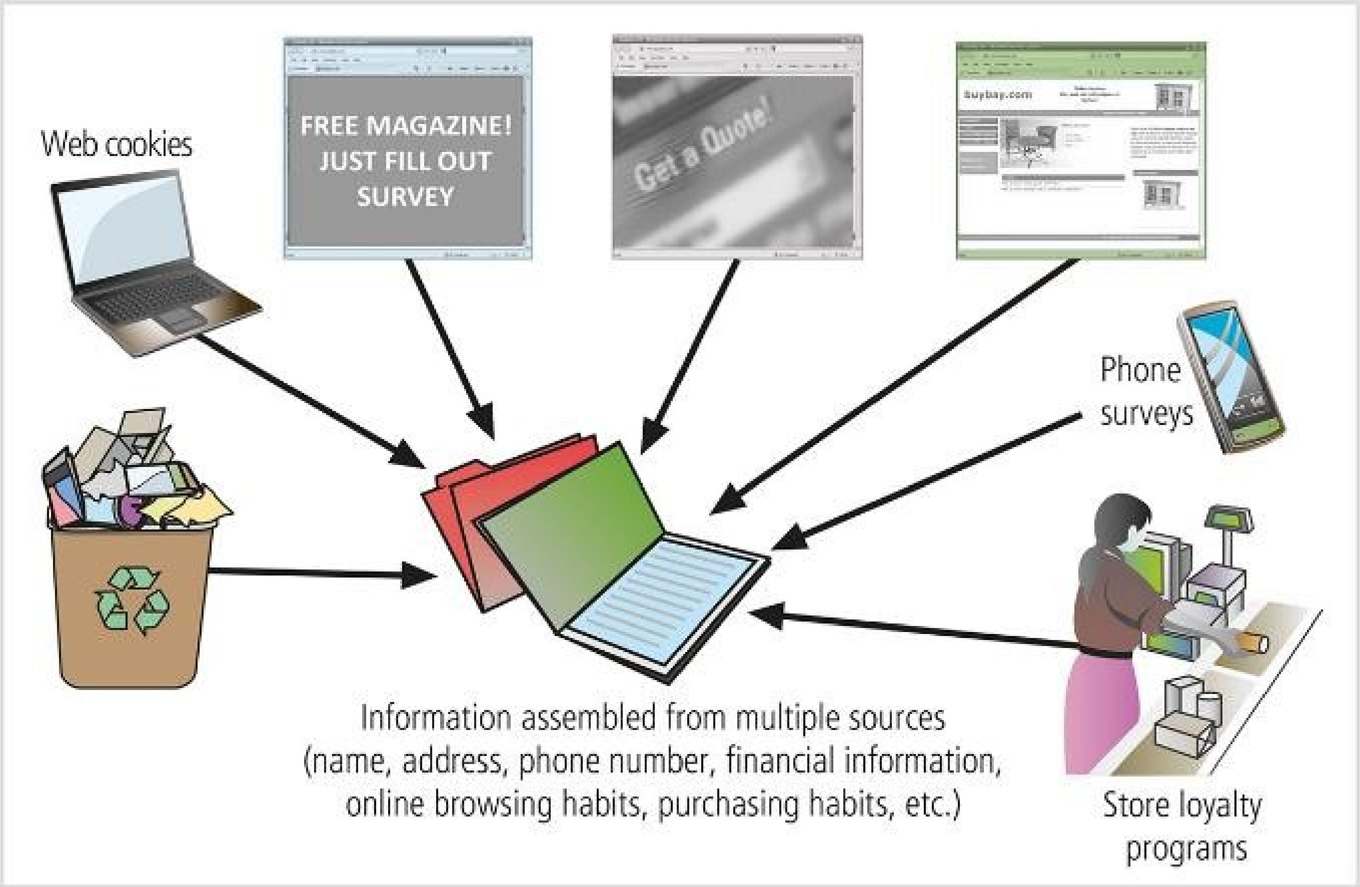

Web cookies
FREE MAGAZINE! JUST FILL OUT SURVEY
Get a Quote!
buybay.com
Phone surveys
Store loyalty programs
Information assembled from multiple sources (name, address, phone number, financial information, online browsing habits, purchasing habits, etc.)

Figure 6-2 Information aggregation

Privacy (2 of 2)

- U.S. Regulations
  - Privacy of Customer Information Section of the common carrier regulation
  - Federal Privacy Act of 1974
  - Electronic Communications Privacy Act of 1986
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA), aka Kennedy-Kassebaum Act
  - Financial Services Modernization Act, or Gramm-Leach-Bliley Act of 1999

Knowledge Check Activity 2

Which of the following is another name for the Financial Services Modernization Act?

a. Gramm-Leach-Bliley Act

b. Hitech Act

c. The HIPAA Act

d. Kennedy-Kassebaum Act

Knowledge Check Activity 2: Answer

Which of the following is another name for the Financial Services Modernization Act?

a. Gramm-Leach-Bliley Act
b. Hitech Act
c. The HIPAA Act
d. Kennedy-Kassebaum Act

Answer: a. Gramm-Leach-Bliley Act

Explanation.

The other choices are all healthcare-related privacy statutes.

Identity Theft (1 of 2)

- Identity theft can occur when someone steals victim’s personally identifiable information (PII) and poses as the victim to conduct actions/make purchases.
- Federal Trade Commission oversees efforts to foster coordination, effective prosecution of criminals, and methods to increase victim’s restitution.
- Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information (Title 18, U.S.C. § 1028).

Identity Theft (2 of 2)

- If someone suspects identity theft, the FTC recommends the following:
  - Place an initial fraud alert: Report to one of the three national credit reporting companies and ask for an initial fraud alert on your credit report.
  - Order your credit reports: Filing an initial fraud alert entitles you to a free credit report from each of the three credit reporting companies. Examine the reports for fraud activity.
  - Create an identity theft report: Filing a complaint with the FTC will generate an identity theft affidavit, which can be used to file a police report and create an identity theft report.
  - Monitor your progress: Document all calls, letters, and communications during the process.

Export and Espionage Laws

- Economic Espionage Act of 1996 (EEA)
- Security and Freedom through Encryption Act of 1999 (SAFE)
- The acts include provisions about encryption that state the following:
  - Reinforce the right to use or sell encryption algorithms, without concern of key registration.
  - Prohibit the federal government from requiring it.
  - Make it not probable cause to suspect criminal activity.
  - Relax export restrictions.
  - Additional penalties for using it in a crime.

U.S. Copyright Law

- Intellectual property was recognized as a protected asset in the United States; copyright law extends to electronic formats.
- With proper acknowledgment, it is permissible to include a “fair use” portion of others’ work as reference.
- U.S. Copyright Office: Web site: www.copyright.gov/.

Knowledge Check Activity 3

Intellectual property includes all of the following **EXCEPT**?

a. The recipe to make Coca-Cola

b. An article from the New York Times

c.

d. The Adventures of Sherlock Holmes (1892)

e. Process to manufacturer an iPhone

Knowledge Check Activity 3: Answer

Intellectual property includes all of the following EXCEPT?

Answer: d. The Adventures of Sherlock Holmes (1892)

This work of fiction is no longer protected by copyright as that has expired.

Financial Reporting

- Sarbanes-Oxley Act of 2002, also known as SOX or the Corporate and Auditing Accountability and Responsibility Act of 2002, is a critical piece of legislation that affects the executive management of publicly traded corporations and public accounting firms.
- SOX seeks to improve the reliability and accuracy of financial reporting and increase the accountability of corporate governance in publicly traded companies.
- It provides penalties for noncompliance ranging from fines to jail terms.

Freedom of Information Act of 1966 (FOIA)

- Allows access to federal agency records or information not determined to be matter of national security.
- U.S. government agencies are required to disclose any requested information upon receipt of written request.
- Some information is protected from disclosure; this act does not apply to state/local government agencies or private businesses/individuals.

Payment Card Industry Data Security Standards (PCI DSS)

- PCI Security Standards Council offers a standard of performance to which organizations processing payment cards must comply.
  - PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.
  - PCI DSS provides a baseline of technical and operational requirements designed to protect account data.
  - PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers.
  - PCI DSS also applies to all other entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD).

PCI DSS Requirements (1 of 2)

PCI DSS Area	PCI DSS Requirement
Build and maintain a secure network and systems	Install and maintain a firewall configuration to protect cardholder data. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect cardholder data	Protect stored cardholder data. Encrypt transmission of card holder data across open, public networks.
Maintain a vulnerability management program	Protect all systems against malware and regularly update antivirus software or programs. Develop and maintain secure systems and applications.

PCI DSS Requirements (2 of 2)

PCI DSS Area	PCI DSS Requirement
Implement strong access control measures	Restrict access to cardholder data by a business need to know. Identify and authenticate access to system components. Restrict physical access to cardholder data.
Regularly monitor and test networks	Track and monitor all access to network resources and cardholder data. Regularly test security systems and processes.
Maintain an information security policy	Maintain a policy that addresses information security for all personnel.

State and Local Regulations

- Federal computer laws are mainly written specifically for federal information systems; they have little applicability to private organizations.
- Information security professionals are responsible for understanding state regulations and ensuring that organization is in compliance with regulations.

International Laws and Legal Bodies

- When organizations do business on the Internet, they do business globally.
- Professionals must be sensitive to the laws and ethical values of many different cultures, societies, and countries.
- Because of the political complexities of relationships among nations and differences in culture, few international laws cover privacy and information security.
- These international laws are important but are limited in their enforceability.

Council of Europe Convention on Cybercrime

- Created international task force to oversee Internet security functions for standardized international technology laws.
- Attempts to improve effectiveness of international investigations into breaches of technology law.
- Well received by intellectual property rights advocates due to emphasis on copyright infringement prosecution.
- Lacks realistic provisions for enforcement.

WTO and the Agreement on Trade-Related Aspects of IP Rights

- The first significant international effort to protect intellectual property rights which outlines requirements for governmental oversight and legislation providing minimum levels of protection for intellectual property.
- Agreement covers five issues:
  - Application of basic principles of trading system and international intellectual property agreements.
  - Giving adequate protection to intellectual property rights.
  - Enforcement of those rights by countries within their borders.
  - Settling intellectual property disputes.
  - Transitional arrangements while a new system is being introduced.

Digital Millennium Copyright Act (DMCA)

- U.S. contribution to international effort to reduce impact of copyright, trademark, and privacy infringement.
- A response to European Union Directive 95/46/EC states the following:
  - Prohibits the circumvention of protections and countermeasures implemented by copyright owners to control access to protected content.
  - Prohibits the manufacture of devices to circumvent protections and countermeasures that control access to protected content.
  - Bans trafficking in devices manufactured to circumvent protections and countermeasures that control access to protected content.
  - Prohibits the altering of information attached or embedded into copyrighted material.
  - Excludes Internet service providers from certain forms of contributory copyright infringementExcludes ISPs from some copyright infringement.

Ethics and Information Security

- Many professional disciplines have explicit rules governing the ethical behavior of members.
- IT and InfoSec do not have binding codes of ethics.
- Professional associations and certification agencies work to maintain ethical codes of conduct.
  - Can prescribe ethical conduct
  - Do not always have the ability to ban violators from practice in field

The Ten Commandments of Computer Ethics: The Computer Ethics Institute

1. Thou shalt not use a computer to harm other people.
2. Thou shalt not interfere with other people’s computer work.
3. Thou shalt not snoop around in other people’s computer files.
4. Thou shalt not use a computer to steal.
5. Thou shalt not use a computer to bear false witness.
6. Thou shalt not copy or use proprietary software for which you have not paid.
7. Thou shalt not use other people’s computer resources without authorization or proper compensation.
8. Thou shalt not appropriate other people’s intellectual output.
9. Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10. Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

Ethical Differences Across Cultures

- Cultural differences create difficulty in determining what is and is not ethical.
- Difficulties arise when one nationality’s ethical behavior conflicts with the ethics of another national group.
- The ethics study in the text supports the finding that different cultures may have different views on what is ethical.

Ethics and Education

- Education is the overriding factor in levelling ethical perceptions within a small population.
- Employees must be trained and kept aware of the expected behaviour of an ethical employee, as well as many other information security topics.
- Proper ethical training is vital to creating informed and a well-prepared system user.

Deterring Unethical and Illegal Behavior

- Three general causes of unethical and illegal behavior: ignorance, accident, intent.
- Deterrence is the best method for preventing an illegal or unethical activity; for example, laws, policies, technical controls.
- Laws and policies only deter if three conditions are present:
  - Fear of penalty.
  - Probability of being apprehended.
  - Probability of penalty being applied.

Deterrents to Illegal or Unethical Behaviour

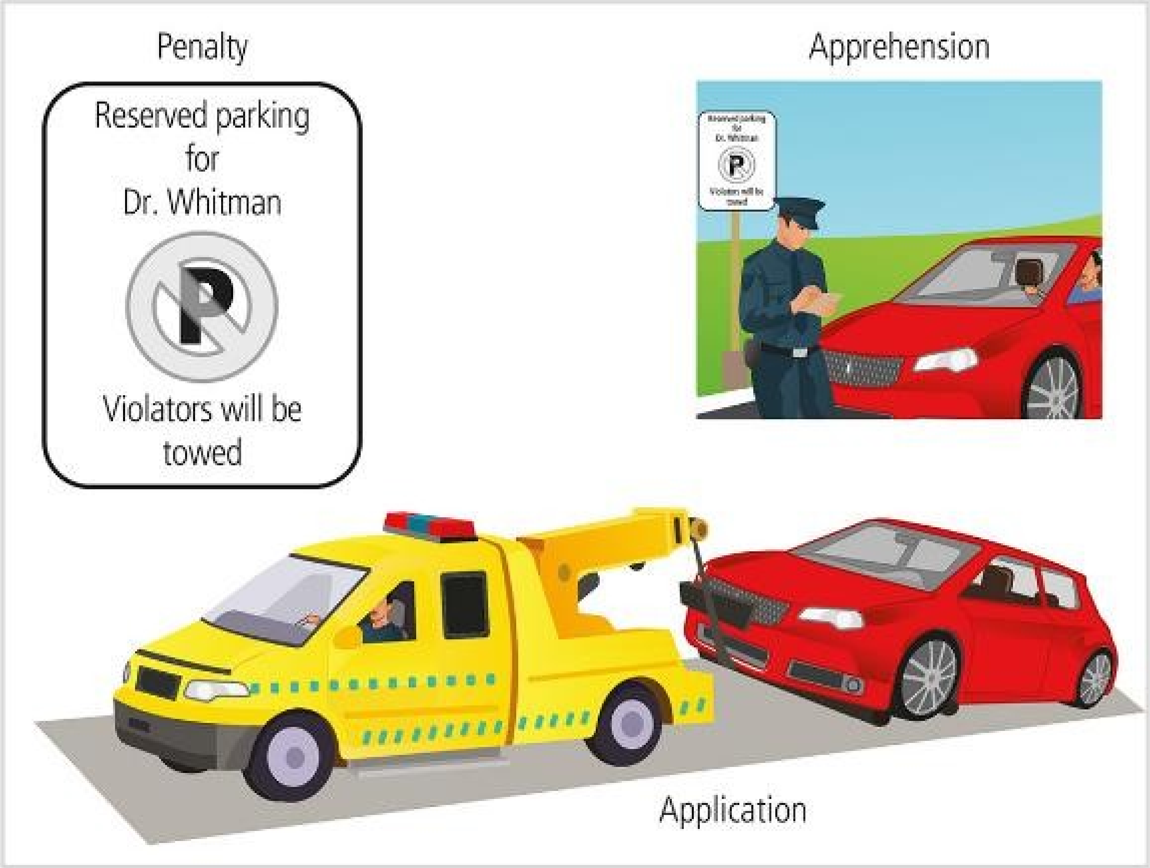


Figure 6-4 Deterrents to illegal or unethical behavior

Codes of Ethics of Professional Organizations

- Many professional organizations have established codes of conduct/ethics.
- Codes of ethics can have a positive effect; unfortunately, many employers do not encourage joining these professional organizations.
- Responsibility of security professionals is to act ethically and according to the policies of the employer, the professional organization, and the laws of society.

Professional Organizations of Interest to Information Security Professionals (1 of 2)

Professional Organization	Web Resource Location	Description and Link to Code of Ethics
ACM	*www.acm.org*	The ACM is the oldest computing society; its code of ethics requires members to perform their duties in a manner befitting an ethical computing professional. *www.acm.org/code-of-ethics*
ISACA	*www.isaca.org*	Promotes a code of ethics for its certification holders, including CISA and CISM. *www.isaca.org/credentialing/code-of-professional-ethics*
ISSA	*www.issa.org*	Professional association of security professionals. *www.members.issa.org/page/CodeofEthics*

Professional Organizations of Interest to Information Security Professionals (2 of 2)

Professional Organization	Web Resource Location	Description and Link to Code of Ethics
(ISC)^2	*www.isc2.org*	Promotes a code of ethics based on four canons for its certification holders, including CISSP and SSCP. *www.isc2.org/Ethics*
SANS GIAC	*www.giac.org*	Promotes a code of ethics based on respect for the public, the certification, and its certification holders, including GIAC and GSE. *www.giac.org/about/ethics*
EC-Council	*www.eccouncil.org*	Promotes a code of ethics for its certification holders, including CCISO and CEH. *www.eccouncil.org/code-of-ethics/*

Major IT & InfoSec Professional Organizations (1 of 3)

- Association of Computing Machinery (ACM)
  - Established in 1947 as "the world's first educational and scientific computing society."
  - Code of ethics contains references to protecting information confidentiality, causing no harm, protecting others' privacy, and respecting others' intellectual property and copyrights.
- International Information Systems Security Certification Consortium, Inc. (ISC)2
  - Non-profit organization focusing on the development and implementation of information security certifications and credentials.
  - Code is primarily designed for the information security professionals who have certification from (ISC)2.
  - Code of ethics focuses on four mandatory canons.

Major IT & InfoSec Professional Organizations (2 of 3)

- SANS (originally System Administration, Networking, and Security Institute)
  - Professional organization with a large membership dedicated to the protection of information and systems.
  - SANS offers a set of certifications called Global Information Assurance Certification (GIAC).
- ISACA (originally Information Systems Audit and Control Association)
  - Professional association with focus on auditing, control, and security
  - Concentrates on providing IT control practices and standards
  - ISACA has a code of ethics for its professionals

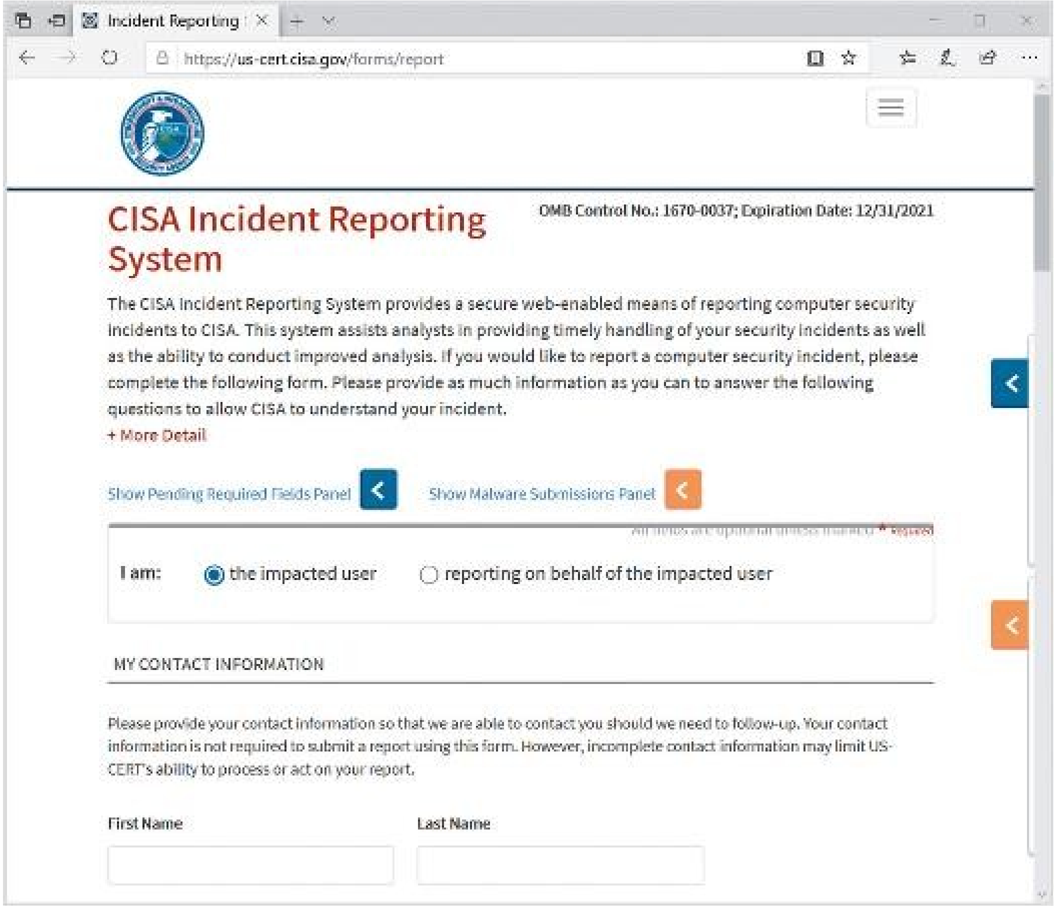
Major IT & InfoSec Professional Organizations (3 of 3)

- Information Systems Security Association (ISSA)
  - Non-profit society of information security (IS) professionals.
  - Primary mission to bring together qualified IS practitioners for information exchange and educational development.
  - Promotes code of ethics similar to (ISC)2, ISACA, and ACM.
- EC-Council
  - Another security certification organization, with more than 220,000 certified professionals in more than 145 countries.
  - Offers a variety of security technical and managerial certifications, building on its renowned Certified Ethical Hacker (CEH) and CCISO certifications.
  - Promotes a 19-point code of ethics for certification holders.

Key U.S. Federal Agencies (1 of 3)

- Department of Homeland Security (DHS)
  - Mission is to protect the citizens as well as the physical and informational assets of the United States.
  - Cybersecurity role extends from its Cybersecurity and Infrastructure Security Agency (CISA), which offers a variety of services to government, industry and the private sector, academia, nonprofit/NGO organizations, and the general public through their services portal.
  - US-CERT provides mechanisms to report phishing and malware.
- U.S. Secret Service
  - In addition to protective services, it is charged with safeguarding the nation’s financial infrastructure and payments system to preserve integrity of the economy.

CISA Incident Reporting System



CISA Incident Reporting System

OMB Control No.: 1670-0037; Expiration Date: 12/31/2021

The CISA Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis. If you would like to report a computer security incident, please complete the following form. Please provide as much information as you can to answer the following questions to allow CISA to understand your incident.

+ More Detail

Show Pending Required Fields Panel

Show Malware Submissions Panel

All fields are optional unless marked * required

I am: ● the impacted user ○ reporting on behalf of the impacted user

MY CONTACT INFORMATION

Please provide your contact information so that we are able to contact you should we need to follow-up. Your contact information is not required to submit a report using this form. However, incomplete contact information may limit US-CERT's ability to process or act on your report.

First Name

Last Name

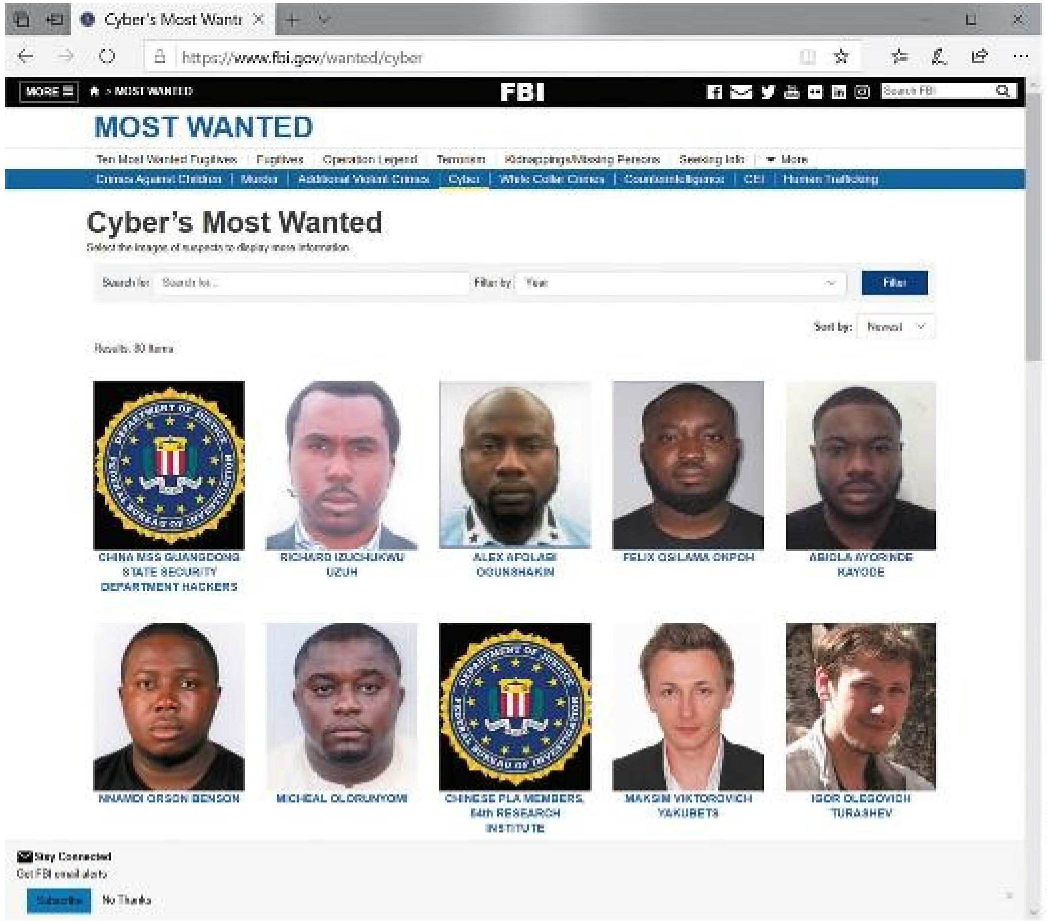
Source: CISA, DHS.

Figure 6-7 CISA incident reporting system

Key U.S. Federal Agencies (2 of 3)

- Federal Bureau of Investigation (FBI)
  - Primary law enforcement agency that investigates traditional crimes and cybercrimes.
  - Key priorities include computer/network intrusions, identity theft, and fraud
  - FBI’s National InfraGard Program
    - Maintains an intrusion alert network
    - Maintains a secure Web site for communication about suspicious activity or intrusions
    - Sponsors local chapter activities
    - Operates a help desk for questions

FBI Cyber’s Most Wanted List



MOST WANTED

Cyber’s Most Wanted

Select the images of suspects to display more information.

Results: 30 Items

CHINA MSS GUANGDONG STATE SECURITY DEPARTMENT HACKERS

RICHARD IZUCHUKWU UZUH

ALEX APOLARI OGUNSHAKIN

FELIX OSILAMA OKPOH

ABIOLA AYORINDE KAYODE

NNAMDI ORSON BENSON

MICHEAL OLORUNYOMI

CHINESE PLA MEMBERS, 54th RESEARCH INSTITUTE

MAKSIM VIKTOROVICH YAKUBETS

IGOR OLEGOVICH TURASHEV

Stay Connected

Get FBI email alerts

Source: FBI.

Figure 6-9 FBI Cyber’s Most Wanted list

Key U.S. Federal Agencies (3 of 3)

- National Security Agency (NSA)
  - The nation's cryptologic organization
  - Responsible for signal intelligence and information assurance (security)
  - Information Assurance Directorate (IAD) is responsible for the protection of systems that store, process, and transmit information of high national value.

Knowledge Check Activity 4

Which U.S. Federal agency is most responsible for developing and using encryption?

a. FBI

b. Secret Service

c. National Institute for Science and Technology

d. National Security Agency

Knowledge Check Activity 4: Answer

Which U.S. Federal agency is most responsible for developing and using encryption?

a. FBI
b. Secret Service
c. National Institute for Science and Technology
d. National Security Agency

Answer: d. National Security Agency

The National Security Agency (NSA) is the nation’s cryptologic organization and is responsible for signal intelligence and information assurance.

Summary (1 of 3)

- Laws are formally adopted rules for acceptable behavior in modern society. Ethics are socially acceptable behavior. The key difference between laws and ethics is that laws carry the authority of a governing body and ethics do not.
- Organizations formalize desired behavior in documents called policies. Policies must be read and agreed to before they are binding.
- Civil law comprises a wide variety of laws that govern a nation or state. Criminal law addresses violations that harm society and is enforced by agents of the state or nation.
- Private law focuses on individual relationships, and public law governs regulatory agencies. Key U.S. laws to protect privacy include the Federal Privacy Act of 1974, the Electronic Communications Privacy Act of 1986, and the Health Insurance Portability and Accountability Act of 1996.

Summary (2 of 3)

- The desire to protect national security, trade secrets, and a variety of other state and private assets has led to the passage of several laws that restrict what information, information management resources, and security resources may be exported from the United States.
- Intellectual property is recognized as a protected asset in this country. U.S. copyright law extends this privilege to published works, including electronic media.
- Studies have determined that people of differing nationalities have varying perspectives on ethical practices with the use of computer technology.
- Deterrence can prevent an illegal or unethical activity from occurring. Deterrence requires significant penalties, a high probability of apprehension, and an expectation that penalties will be enforced.

Summary (3 of 3)

- As part of an effort to encourage ethical behavior, many professional organizations have established codes of conduct or codes of ethics that their members are expected to follow.
- Several U.S. federal agencies are responsible for protecting American information resources and investigating threats against them.

Self-Assessment

- In this module, you learned about ethics across different cultures.
- How do you feel about the situation that can occur when the same behavior might be considered ethical in one culture but could be thought of as unethical or even illegal in another culture? Do you know of a situation like that?
- How do you feel about actions that are consider ethical in one part of a nation but would be unethical or even illegal in another part of the same nation?