

Data Security and Privacy

Chapter 3: Legal, Ethical, and Professional Issues in Data Security

Introduction

- You must understand scope of an organization's legal and ethical responsibilities
- To minimize liabilities/reduce risks, the data security practitioner must:
 - Understand current legal environment
 - Stay current with laws and regulations
 - Watch for new issues that emerge

Law and Ethics in Information Security

- Laws:
 - rules that mandate or prohibit certain societal behavior
- Ethics:
 - define socially acceptable behavior
- Cultural mores:
 - fixed moral attitudes or customs of a particular group; ethics based on these
- Laws carry sanctions of a governing authority; ethics do not

Organizational Liability and the Need for Counsel

- **Liability:** legal obligation of an entity extending beyond criminal or contract law; includes legal obligation to make restitution
- **Restitution:** to compensate for wrongs committed by an organization or its employees
- **Due care:** insuring that employees know what constitutes acceptable behavior and know the consequences of illegal or unethical actions
- **Due diligence:** making a valid effort to protect others; continually maintaining level of effort
- **Jurisdiction:** court's right to hear a case if the wrong was committed in its territory or involved its citizenry
- **Long arm jurisdiction:** right of any court to impose its authority over an individual or organization if it can establish jurisdiction

Policy versus Law

- Policies:
 - body of expectations that describe acceptable and unacceptable employee behaviors in the workplace
- Policies function as laws within an organization; must be crafted carefully to ensure they are complete, appropriate, fairly applied to everyone
- Difference between policy and law:
 - ignorance of a policy is an acceptable defense
- Criteria for policy enforcement:
 - Dissemination (distribution)
 - Review (reading)
 - Comprehension (understanding)
 - Compliance (agreement)
 - Uniform enforcement

Types of Law

- Civil:
 - governs nation or state; manages relationships/conflicts between organizational entities and people
- Criminal:
 - addresses violations harmful to society; actively enforced by the state
- Private:
 - regulates relationships between individuals and organizations(family law, commercial law, and labor law)
- Public:
 - regulates structure/administration of government agencies and relationships with citizens, employees, and other governments(criminal, administrative, and constitutional law)

Relevant U.S. Laws

- United States has been **a leader** in the ***development*** and ***implementation*** of information security legislation
- **Implementation** of information security legislation **contributes** to a **more reliable** business environment and a **stable** economy
- U.S. has demonstrated understanding of problems facing the information security field; has **specified penalties** for individuals and organizations failing to follow requirements set forth in U.S. civil statutes

Area	Act	Date	Description
Telecommunications	Telecommunications Deregulation and Competition Act of 1996—Update to Communications Act of 1934 (47 USC 151 et seq.)	1934	Regulates interstate and foreign telecommunications (amended 1996 and 2001)
Freedom of information	Freedom of Information Act (FOIA)	1966	Allows for the disclosure of previously unreleased information and documents controlled by the U.S. government
Privacy	Federal Privacy Act of 1974	1974	Governs federal agency use of personal information
Copyright	Copyright Act of 1976—Update to U.S. Copyright Law (17 USC)	1976	Protects intellectual property, including publications and software
Cryptography	Electronic Communications Privacy Act of 1986 (Update to 18 USC)	1986	Regulates interception and disclosure of electronic information; also referred to as the Federal Wiretapping Act
Access to stored communications	Unlawful Access to Stored Communications (18 USC 2701)	1986	Provides penalties for illegally accessing stored communications (such as e-mail and voicemail) stored by a service provider
Threats to computers	Computer Fraud and Abuse Act (also known as Fraud and Related Activity in Connection with Computers) (18 USC 1030)	1986	Defines and formalizes laws to counter threats from computer-related acts and offenses (amended 1996, 2001, and 2006)
Federal agency information security	Computer Security Act of 1987	1987	Requires all federal computer systems that contain classified information to have security plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems
Trap and trace restrictions	General prohibition on pen register and trap and trace device use; exception (18 USC 3121 et seq.)	1993	Prohibits the use of electronic "pen registers" and trap and trace devices without a court order
Criminal intent	National Information Infrastructure Protection Act of 1996 (update to 18 USC 1030)	1996	Categorizes crimes based on defendant's authority to access a protected computer system and criminal intent
Trade secrets	Economic Espionage Act of 1996	1996	Prevents abuse of information gained while employed elsewhere
Personal health information protection	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	1996	Requires medical practices to ensure the privacy of personal medical information
Encryption and digital signatures	Security and Freedom through Encryption Act of 1997	1997	Affirms the rights of persons in the United States to use and sell products that include encryption and to relax export controls on such products
Intellectual property	No Electronic Theft Act Amends 17 USC 506(a)—copyright infringement, and 18 USC 2319—criminal infringement of copyright (Public Law 105-147)	1997	Amends copyright and criminal statutes to provide greater copyright protection and penalties for electronic copyright infringement

Privacy

- One of the hottest topics in information security
- Is a “state of being free from unsanctioned intrusion”
- Ability to aggregate data from multiple sources allows creation of information databases previously impossible
- The number of statutes addressing an individual’s right to privacy has grown
- US Regulations
 - Financial Services Modernization Act, or Gramm-Leach-Bliley Act of 1999

Privacy (cont'd.)

- Identity Theft
 - Federal Trade Commission: “occurring when someone uses your personally identifying information (your name, Social Security number, or credit card number), without your permission, to commit fraud or other crimes”
 - Fraud And Related Activity In Connection With Identification Documents, Authentication Features, And Information
- If someone suspects identity theft
 - Report to the three dominant consumer reporting companies that your identity is threatened
 - Close compromised account
 - Dispute accounts opened without permission
 - Register your concern with the FTC
 - Report the incident to either your local police or police in the location where the identity theft occurred

GDPR and e-PR

- **What is GDPR?**
 - stands for General Data Protection Regulation: created to improve data privacy.
- **What is ePR?**
 - stands for e-Privacy Regulation: for electronic communications and the right of confidentiality. It isn't just about cookies, it concerns electronic communications and the right of confidentiality, data/privacy protection and more.
- **When is GDPR enforced?** 25th of May 2018
- **When is ePR enforced?** Nobody knows yet
- GDPR applies to data subjects within the European Union (EU). It gives control to EU data subjects in regards to how their data is processed, stored, or transmitted. The ripple effect of GDPR reaches organizations outside of the EU, many of which are based in the U.S.

some key to ensure your organization is ready for GDPR:

- **Identity and Access Management (IDAM)**
 - limit access to personal data for **authorized employees**.
 - Principles in IDAM: **separation of duties** and **least privilege**,
 - help ensure that employees have access only to information or systems applicable to their job function.
 - privacy training should be available individuals to ensure that the intended purpose for the collection of personal data is maintained.
- **Data Loss Prevention (DLP)**
 - helps prevent the loss of personal data.
 - Technical safeguards are critical in preventing a breach.
 - Incorporating DLP controls adds a layer of protection by restricting the **transmission of personal data** outside the network.
- **Encryption & Pseudonymization**
 - Pseudonymization is the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information: include field **level encryption** in databases, encryption of entire data stores at rest, as well as encryption for data in use and in transit.

some key to ensure your organization is ready for GDPR:

- **Incident Response Plan (IRP):**
 - address phases such as: **preparation, identification, containment, eradication, recovery and lessons learned.**
 - In case of a data breach that involves personal information, an organization must notify the **Data Protection Authority** within 72 hours; and Communicate high-risk breaches to affected data subjects without undue delay.
- **Third-Party Risk Management**
 - GDPR cybersecurity compliance is important for third-party relationships as it is internally for an organization as long as those third parties process, store, or transmit personal data of EU data subjects.
- **Policy Management**
 - policy must receive enterprise-wide buy-in in order to manage and update data security controls in an always changing cybersecurity environment.
organizational policy acknowledgment and training ensures policies are properly communicated and understood.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Protects the confidentiality and security of health care data by establishing and enforcing standards and by standardizing **electronic data interchange**
- **Consumer** control of medical information
- **Boundaries** on the **use** of medical information
- **Accountability** for the privacy of private information
- Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
- Security of health information

Financial Reporting

- Seeks to improve reliability and accuracy of financial reporting and increase the accountability of corporate governance
- Penalties for noncompliance range from fines to jail terms
- Reliability assurance will require additional emphasis on confidentiality and integrity

State and Local Regulations

- Restrictions on organizational computer technology use exist at international, national, state, local levels
- Information security professional responsible for understanding state regulations and ensuring organization is **compliant with regulations**

International Laws and Legal Bodies

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

European Council Cyber-Crime Convention

- Establishes international task force overseeing 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

Agreement on Trade-Related Aspects of Intellectual Property Rights

- Created by World Trade Organization (WTO)
- 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 in their own territories
 - Settling intellectual property disputes
 - Transitional arrangements while 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
- Prohibits
 - Circumvention of protections and countermeasures
 - Manufacture and trafficking of devices used to circumvent such protections
 - Prohibits altering information attached or imbedded in copyrighted material
- Excludes ISPs from some copyright infringement

Ethics and Information and Data Security

- Many Professional groups have explicit rules governing ethical behavior in the workplace
- IT and IT security do not have binding codes of ethics
- Professional associations and certification agencies work to establish codes of ethics (ethical conduct)

Offline

The Ten Commandments of Computer Ethics¹³

From 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 Data Privacy Principles:

1. Comply with national data protection or privacy law, national contract law, and other legal requirements or regulations relating to data privacy.
2. Comply with current security standards to protect stored personal data from illegitimate or unauthorized access or from accidental access, processing, erasure, loss or use.
3. Implement an **easily** perceptible, accessible and comprehensible privacy policy with information on **who** is in charge of data privacy and **how** this person can be individually contacted, **why and which** personal data are collected, **how** these data are used, **who** will receive these data, **how** long these data are stored, and **whether and which** data will be deleted or rectified upon request.
4. Instruct employees to comply with such privacy policies and avoid activities that enable or facilitate illegitimate or unauthorized access in terms of IDPPs.
5. Do not use or divulge any customer data (except for **statistical analysis and when the customer's identity remains anonymous**), unless the company is obliged to do so by law or the customer agrees to such use or circulation.
6. Do not collect customer data if such collection is unnecessary or excessive.

Ethical Data Privacy Principles(cont'):

7. Use or divulge customer data in a fair way and only for a purpose related to activities of the company.
8. Do not outsource customer data to third parties unless they also comply with standards comparable to these IDPPs.
9. Announce data breaches relating to sensitive data.
10. Do not keep personal data for longer than necessary.
11. Do not transfer personal data to countries with inadequate or unknown data protection standards unless the customer is informed about these standards being inadequate or unknown and agrees to such a transfer.
12. In the case of (or absence) a contract between the company and the customer in which the customer commits to pay for services or goods:
 - Inform the customer individually in the event of a data breach, or about which specific data are stored, and delete such data upon request unless applicable laws or regulations require the company to continue storing such data.
 - Do not use or divulge content-related personal data without the customer's **explicit, separate and individual consent**.

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 ethics of another national group
- Scenarios are grouped into:
 - Software License Infringement
 - Illicit Use
 - Misuse of Corporate Resources
- Cultures have different views on the scenarios

Ethics and Education

- Overriding factor in levelling ethical perceptions within a small population is education
- Employees must be trained in expected behaviors of an ethical employee, especially in areas of information security
- Proper ethical training is vital to creating informed, well prepared, and low-risk system user

Detering Unethical and Illegal Behavior

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

Major IT Professional Organizations

- Association of Computing Machinery (ACM)
 - “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
- International Information Systems Security Certification Consortium, Inc. (ISC)²
 - focusing on development and implementation of information security certifications and credentials
- System Administration, Networking, and Security Institute (SANS)
 - dedicated to protection of information and systems
- Information Systems Audit and Control Association (ISACA)
 - focus on auditing, control, and security
- Information Systems Security Association (ISSA)
 - bring together qualified IS practitioners for information exchange and educational development

Key U.S. Federal Agencies

- Department of Homeland Security (DHS)
 - to protect people, physical and informational assets of the US
- Federal Bureau of Investigation's National InfraGard Program
 - Maintains an intrusion alert network, a secure Web site for communication about suspicious activity or intrusions
- National Security Agency (NSA)
 - the Nation's cryptologic organization
 - Responsible for signal intelligence and information system security
- U.S. Secret Service
 - protective services, charged with the detection and arrest of persons committing a federal offense relating to computer fraud or false identification