Lecture 12: Law and Ethics

EECS711 Security Management & Audit

Objectives

- Identify major national and international laws that relate to the practice of InfoSec
- Describe the role of culture as it applies to ethics in InfoSec
- Discuss current laws, regulations, and relevant professional organizations

Law and Ethics in InfoSec

- **Laws** – rules adopted and enforced by governments to codify expected behavior in modern society
- **Ethics** – socially acceptable behaviors that conform to the widely held principles of the members of that society
  - **Cultural mores –** relatively fixed moral attitudes or customs of a societal group
  - Some ethics are thought to be universal
    - Example: murder, theft, and assault are actions that deviate from ethical/legal codes in most cultures

InfoSec and the Law

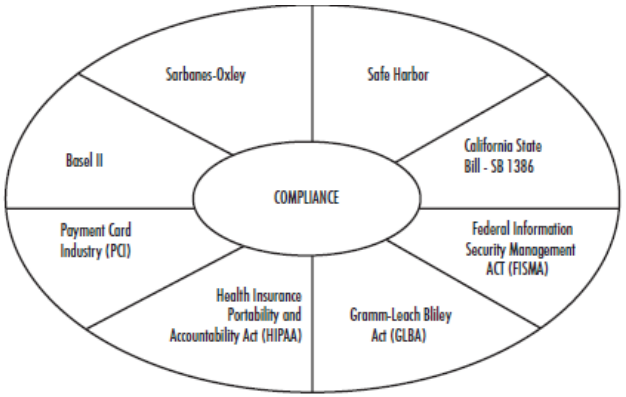
- InfoSec professionals must possess a rudimentary grasp of the legal framework
  - **Civil Law**
    - Laws pertaining to relationships between and among individuals and organizations
  - **Criminal Law**
    - Addresses violations harmful to society and is enforced and prosecuted by the state
  - **Tort Law – a** subset of **Civil Law**
    - Allows individuals to seek redress in the event of personal, physical, or financial injury

InfoSec and the Law

- Legislation affecting individuals in workplace
  - **Private Law**
    - Regulates relationships among individuals and among individuals and organizations
    - Includes family law, commercial law, and labor law
  - **Public Law**
    - Regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments
    - Includes criminal, administrative, and constitutional law

Relevant U.S. Laws

- **InfoSec legislation and compliance**
  - Its development promotes the general welfare and creates a stable environment for a solid economy



  - The U.S. federal government has led the development and implementation of InfoSec legislation
    - Prevent misuse and exploitation of information and information technology
      - Read Table 12-1
    - E-Commerce, communication, copyright, information disclosure, illegal access and privacy, PHI protection, identity theft, computer fraud, spam, terrorism, ….

General Computer Crime Laws

- **Computer Fraud and Abuse Act (CFAA)**
  - The **cornerstone** of many computer-related federal laws
    - Enacted by Congress in 1986; Amended several time later
  - It makes the **unauthorized access** to a very wide range of computer systems a **federal felony**
    - Include systems of federal government, financial institutions, and any protected system used in interstate commerce
      - Intentionally access a protected computer without or exceeding authorization AND obtain anything of value, cause damages, further intended fraud
      - Knowingly defraud protected computers, traffics, …
      - Unauthorized access to computers of government of US
      - With intention to extort from person, firm, association, …

General Computer Crime Laws

- CFAA was amended in the **National Information Infrastructure Protection Act** in 1996
  - Categorizes crimes based on defendant's authority to access a protected computer systems and criminal intent
  - **Increases penalties** for selected crimes based on
    - the value of information obtained
    - the purpose of offense
      - For purposes of commercial advantage
      - For private financial gain
      - Or in furtherance of a criminal act

General Computer Crime Laws

- CFAA was amended in the **USA PATRIOT Act** in 2001
  - To combat terrorism-related activities
    - Defines stiffer penalty for prosecution of terrorist crimes
    - Extend jurisdiction of secret services to remove obstacles
      - Authority to intercept voice comm. in computer hacking investigations
      - Obtain voice mail and stored voice communications
      - Emergency disclosures by communication providers
      - Intercept the communications of computer trespassers
      - Nationwide search warrants for email
      - Deterrence and prevention of cyberterrorism
      - Development and support of cybersecurity forensic capabilities
    - Parts of the Patriot Act expired in 2015, but restored and renewed through the USA Freedom Act in 2015
      - E.g., the 2015 San Bernardino case

General Computer Crime Laws

- **Computer Security Act (CSA)** of 1987
  - First attempt to **protect federal computer systems** by establishing minimum acceptable security practices
    - NSA and National Bureau of Standard develop standards and guidelines to secure federal computer systems
    - Computer System Security and Privacy Advisory Board within DOC lead the effort
    - Amended the Federal Property and Administrative Services Act of 1949 to distribute the standards and guidelines
    - Requires **mandatory** training in computer security awareness and accepted computer security practice for all federal employees

Privacy Laws

- **Privacy** is the “state of being free from unsanctioned intrusion”
  - Defined in the Fourth Amendment of the U.S. Constitution
- Need privacy laws and regulations
  - Many organizations collect, trade, and sell personal information as a commodity
    - Who can use individual and business’s information?
    - Under which conditions?
    - Who holds what responsibilities?
  - The number of statutes addressing individual privacy rights has grown

Who should Protect?

- **Privacy of Customer Information**
  - Section 222 in Title 47 of the United States Code
  - **Regulates public carriers' use of private data**
    - Any proprietary information shall be used for providing services, and not for any marketing purposes
    - Carriers cannot disclose information except when necessary to provide services, or by customer request
      - Then, disclosure is restricted to that customer's info only
    - Permit the use of **aggregate information**
      - The same information is provided to all common carriers for fair competition
      - Pay attention to the re-identification problem

Who should Protect?

- **Federal Privacy Act** of 1974
  - **Regulates government's use of private information**
    - Government agencies are responsible if any portion of individuals' and businesses' information is released without permission
    - Below entities are exempt from some of the regulations:
      - Bureau of the Census
      - National Archives and Records Administration
      - U.S. Congress
      - Comptroller General
      - Certain court orders
      - Credit agencies

Who should Protect?

- **Health Insurance Portability and Accountability Act**
  - **HIPAA** is also known as the Kennedy-Kassebaum Act (1996)
  - **Regulates all healthcare organizations for protection of electronic protected health information (ePHI)**
    - Protect the confidentiality and security of healthcare data by establishing and enforcing standards and by standardizing electronic data interchange
    - Organizations are required to comply with HIPAA by 2003
      - Hospitals; covered healthcare providers; health plans; health clearinghouses; medical prescription drug card sponsors
    - Fail to comply incurs stiff penalties
      - $25,000 fine and/or 10-year imprisonment for misusing client information

Who should Protect?

- **HIPAA**
  - HIPAA has five fundamental **privacy principles**
    1. Consumer control of medical information
    2. Boundaries on the use of medical information
    3. Security of health information
       - Establishes appropriate safeguards
    4. Accountability for the privacy of private information
       - With civil and criminal penalties
    5. Balance of public responsibility for the use of medical information for the greater good measured against impact to the individual
       - To protect public health

Who should Protect?

- **HIPAA**
  - HIPAA requires Health and Human Services (HHS) to development security standards
  - **HIPAA Security Rule**
    - Requires organizations to use InfoSec mechanisms, policies and procedures to protect PHI
      - Mandates specific outcomes
      - Specifies process and procedural requirements: administrative, physical, technical safeguards
  - **HIPAA Privacy Rule**
    - Restricts the dissemination and distribution of private health information without documented consent

Who should Protect?

- **American Recovery and Reinvestment Act** of 2009
  - Was designed to provide a response to the economic crisis in the U.S.
  - Enacted as part of ARRA was the **HITECH Act**
    - **Health Information Technology for Economic and Clinical Health Act**
    - Significantly increases the penalty amount for HIPAA violations
    - HIPAA and HITECH require that covered entities **notify information owners of breaches**

Who should Protect?

- **Gramm-Leach Bliley Act (GLBA)** of 1999
  - Requires all **financial institutions** to create, implement and disclose **policies** to protect private information from foreseeable threats
    - Affects banks, securities firms, and insurance companies
      - How they share nonpublic personal information
      - How customers can request information not be shared with third parties
    - Ensures privacy policies in effect in an organization are
      - Fully disclosed when a customer initiates a business relationship
      - Distributed annually for the duration of the professional association

Who should Protect?

- **Payment Card Industry Data Security Standard (PCI DSS)**
  - A set of **industry standards** to reduce credit card fraud
    - Created by the Payment Card Industry Standards Council
    - Mandated for **ALL organizations that handle credit, debit, and specialty payment cards**
      - Include assess, remediate, and report steps
      - e.g., organizations that do not comply with PCI must submit a report on compliance (ROC) and a remediation plan to Visa
  - PCI DSS includes three sub-standards:
    - PCI Data Security Standard
    - PIN Transaction Security Requirements
    - Payment Application Data Security Standard

Who should Protect?

- **Payment Card Industry Data Security Standard (PCI DSS)**
  - **Build and Maintain a Secure Network**
    - Install firewall; Not use vendor defaults for passwords/parameters
  - **Protect Cardholder Data**
    - Protect stored data; Encrypt transmission across open networks
  - **Maintain a Vulnerability Management Program**
    - Use and update antivirus programs
    - Develop secure systems and applications
  - **Implement Strong Access Control Measures**
    - Restrict access to data; Assign a unique ID
  - **Regularly Monitor and Test Networks**
    - Track and monitor all access; Test security systems
  - **Maintain an Information Security Policy**

What is Protected?

- **Electronic Communications Privacy Act** of 1986
  - A collection of statutes that regulates the interception of wire, electronic, and oral communications
    - Unauthorized access is a **federal felony**
  - Protects the contents of electronic communications
    1. Interception and disclosure of wire, oral, and electronic communications
    2. Manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices
    3. Confiscation of wire, oral, or electronic communication intercepting devices

What is Protected?

4. Evidentiary use of intercepted wire or oral communications
5. Authorization for interception of wire, oral, or electronic communications
6. Authorization for disclosure and use of intercepted wire, oral, or electronic communications
7. Procedure for and reports concerning interception of wire, oral, or electronic communications
8. Injunction against illegal interception

– InfoSec professionals must ensure that the **authorization** they receive from customers are broad and specific enough to mitigate criminal liability under ECPA

What is Protected?

- **Economic Espionage Act (EEA)** of 1996
  - Attempts to protect trade secrets (intellectual property and competitive advantage) from
    - Spy from foreign government or between two US companies; disgruntled former employees
- **Security and Freedom through Encryption Act** of 1997
  - Guides on the use of encryption and institutes measures of public protection from government intervention
    - Relaxes export restrictions by amending EEA
    - Additional penalty for the use of encryption in criminal act
    - Individual's right to use and sell encryption algorithms
    - Prohibits federal government from requiring the use of encryption for contracts, grants, …

What is Protected?

	Trade secret	Copyright	Patent
Protects	Secret information	Expression of idea	Invention
Object made public	No	Yes: intention is to promote	Design filed at patent office
Requirement to distribute	No	Yes	No
Ease of filing	No filing	Very easy, do-it-yourself	Very complicated; specialist lawyer suggested
Duration	Indefinite	Life of human originator or 75 years of company	19 years
Legal protection	Sue if secret improperly obtained	Sue if copy sold	Sue if invention copied
Examples	Source code	Object code, documentation	Hardware

What is Protected?

- **U.S. Copyright Law**
  - Extends protection to intellectual property (words published in electronic formats)
    - Proper acknowledgement to copyright owner
    - The **doctrine of fair use** allows materials for activities for educational or non-profit purposes
- **Digital Millennium Copyright Act (DMCA)** of 1996
  - Criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works
- **Stop Online Piracy Act (SOPA)** of 2011
  - Require ISPs/search sites to block sites that have infringed works

What should be Disclosed?

- **Freedom of Information Act (FOIA)** of 1966
  - **Applies only to federal agencies**
    - All federal agencies are required to disclose records requested in writing by any person
    - Agencies may withhold information pursuant to nine **exemptions** and three **exclusions** contained in the statute
    - Does not create a right of access to records held by Congress, the courts, or by state or local government agencies

What should be Disclosed?

- **Sarbanes-Oxley Act (SOX)** of 2002
  - Affects **publicly traded corporations**
    - Issues exposed in financial scandals at Enron, WorldCom, …
  - Designed to enforce accountability for the **financial reporting and record-keeping**
    - Requires the CEO and CFO assume direct and personal accountability for the completeness and accuracy of financial reporting and record-keeping systems
    - CIOs and CISOs are responsible for the security, accuracy, and reliability of the systems that manage and report the financial data
      - Compliance with SOX should be assessed

The Future of U.S. InfoSec Laws

- Several bills fight their way through U.S. Congress
  - To protect consumers' personal information
    - Data Security Act of 2010
  - To respond to a security breach
    - Data Security and Breach Notification Act of 2010
  - To enhance the security of critical infrastructure
    - Cybersecurity Act of 2012
  - All of the above bills failed to pass
- It is expected that similar legislation will inevitably make its way through Congress

International Laws

- **Organizations with Internet business** should also consider international laws
  - Governed by international treaties and trade agreements
  - Many domestic laws and customs do not apply to international trade
  - International security bodies and regulations are sometimes limited in scope and enforceability

International Laws

- **European Council Cybercrime Convention** (2001)
  - Drafted by the Council of Europe
  - Standardize technology laws across international borders
    - Empowers an international task force to oversee a range of Internet security functions
    - **Protects IP rights**: provides for copyright infringement prosecution
  - Lacks enforcement provisions
    - Aims to simplify the acquisition of information for law enforcement agents in certain types of international crimes as well as during the extradition process

International Laws

- **Directive 95/46/EC of the European Parliament**
  - The European Union equivalents to the DMCA
    - Increase individual rights to process and freely move personal data
  - **Database Right**
    - The United Kingdom implementation of this directive
    - UK Law: Copyright and Rights in Databases Regulations 1997

International Laws

- **Computer Offences of the Criminal Code Act 1995**
  - Australia law for high tech crimes
  - Includes:
    - Data system intrusions (such as hacking)
    - Unauthorized destruction or modification of data
    - Actions intended to deny service of computer systems to intended users
      - DoS and DDoS attacks
    - The creation and distribution of malware

State and Local Regulations

- Each state and locality have laws and regulations
  - Regard the use of computer technology
  - Example:
    - The state of Georgia passed the Georgia Computer Systems Protection Act in 1991
    - Georgia legislature also passed the Georgia Identity Theft Law in 1998
    - Kansas Statute 21-3704: Theft of services
    - Kansas Statute 21-3755: Computer crime; computer password disclosure; computer trespass

Policy vs. Law

- Policies function like laws
  - Carefully crafted and fairly applied
- Key difference – ignorance of policy is a viable defense
  - Policies must be:
    - Distributed to all individuals who are expected to comply with them
    - Readily available for employee reference
    - Easily understood, with multilingual translations and translations for visually impaired or low-literacy employees
    - Acknowledged by the employee
    - Uniformly enforced for all employees

Ethics

- **Ethics**
  - An objectively defined standard of “right” and “wrong”
  - Based on cultural mores: relatively fixed moral attitudes or customs of a societal group
  - **Key difference** between ethics and law – law carries the sanction of a governing authority and ethics do not
- **Ten Commandments of Computer Ethics**
  - Created in 1992 by the Computer Ethics Institute
  - The CISSP uses this as a foundation for its ethics rules

The Ten Commandments of Computer Ethics

Written by the Computer Ethics Institute

by 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.

Computer Ethics Institute

Ethics in InfoSec

- **Ethical frameworks**
  - Normative ethics
    - Study of what makes actions right or wrong – moral theory
    - Ethical action – how should people act?
  - Meta-ethics
    - Study of the meaning of ethical judgments and properties – what is right?
  - Descriptive ethics
    - Study of choices that have been made by individuals in the past
    - Comparative ethics to study people's beliefs – what do others think is right?
  - Applied ethics
    - Applies moral codes to actions drawn from realistic situations – how to use ethics in practice?
  - Deontological ethics
    - Study of the rightness or wrongness of intentions and motives
    - Based on the action's adherence to a rule

Ethical Standards

- **Ethical standards**
  - Utilitarian approach
    - Results in the most good or least harm
  - Rights approach
    - Best protects and respects the moral rights
  - Fairness or justice approach
    - Having outcomes that regard all human beings equally
  - Common good approach
    - This approach tends to focus on the common welfare
  - Virtue approach
    - Ethical actions ought to be consistent with so-called ideal virtues – honesty, courage, compassion, integrity, fairness…

Ethics in InfoSec

- **InfoSec is responsible** for stopping unethical and illegal behavior
  - Ignorance
  - Accident
  - Intent
- **Deterrence** is the best method
  - Policies and laws work only when
    - Fear of penalty
    - Probability of being caught
    - Probability of penalty being administered
  - Education and training

Ethics in InfoSec

- **Ethics Education**
  - The overriding factor in leveling the ethical perceptions within a small population
  - Employees must be trained and kept up to date on InfoSec topics
    - The expected behaviors of an ethical employee
    - Unethical or even illegal behaviors
  - Proper ethical and legal training is vital to creating an informed, well-prepared, and low-risk system user

Example of Ethical Scenario

- **Training based on Ethical Scenario**
  - Using practical situations in training ethical choices

Table 3. An Example of Scenario

A student suspected and found a loophole in the university computer's security system that allowed him to access other students' records. He told the system administrator about the loophole, but continued to access others' records until the problem was corrected 2 weeks later. A. The student's action in searching for the loophole was B. The student's action in continuing to access others' records for 2 weeks was C. The system administrator's failure to correct the problem sooner was
1) very ethical 2) ethical 3) somewhat ethical 4)questionable 5) somewhat unethical 6) unethical 7) very unethical

Professional Organizations

- Professional organizations have established codes of conduct and/or **codes of ethics**
  - Can have a positive effect on an individual's judgment regarding computer use
  - Employers should recommend employees to get certification or accreditation
- **Association for Computing Machinery (ACM)**
  - World's first educational and scientific computing society
  - **ACM's code of ethics** requires members to perform their duties in a manner befitting an ethical computing professional

Professional Organizations

- Contains specific references to protecting the confidentiality of information, causing no harm, protecting the privacy of others, and respecting intellectual property of others

- **International Information Systems Security Certification Consortium $(ISC)^2$**
  - InfoSec certifications and credentials
  - Code of Ethics:
    - Protect society, the commonwealth, and the infrastructure
    - Act honorably, honestly, justly, responsibly, and legally
    - Provide diligent and competent service to principals
    - Advance and protect the profession

Professional Organizations

- **SANS** (System Administration, Networking, and Security Institute)
  - Research and education cooperative organization
  - SANS Global Information Assurance Certification requires:
    - Respect for the public
    - Respect for the certification
    - Respect for my employer
    - Respect for myself
- **Information Systems Audit and Control Association (ISACA)**
- **Information Systems Security Association (ISSA)**

Organizational Liability

- **Organizations are liable** to (employees') wrongful act
  - Even when no law or contract has been breached
  - Liability includes an obligation to make payment or restitution
  - An organization increases its liability
    - If it refuses to take measures to make sure employees know what is acceptable and what is not
  - Any court can impose its authority if the act was committed in its territory or involve its citizenry
    - Within its *jurisdiction* – a court's right to hear a case

Key Law Enforcement Agencies

- **Organizations may need assistance**
  - **Local law enforcement**
    - Capable of handling physical security threats or employee problems
  - Key **federal agencies** are charged with the protection of U.S. information resources
    - **FBI:** InfraGard organization
      - www.infragard.org
      - Missouri – Kansas City Members Alliance
    - **Department of Homeland Security (DHS):** National Protection and Programs Directorate
    - **NSA: IAD, CAE/IAE centers**
    - **U.S. Secret Service**

Managing Investigations

- How to investigate a suspicious violation?
  - **Digital forensics –** methodical techniques to present evidence of crimes to a court
    - Preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis
    - **Evidentiary material (EM)** – any information that could potentially support the organization's legal-based or policy-based case against a suspect
    - **E-discovery** – the identification and preservation of EM related to a specific legal action

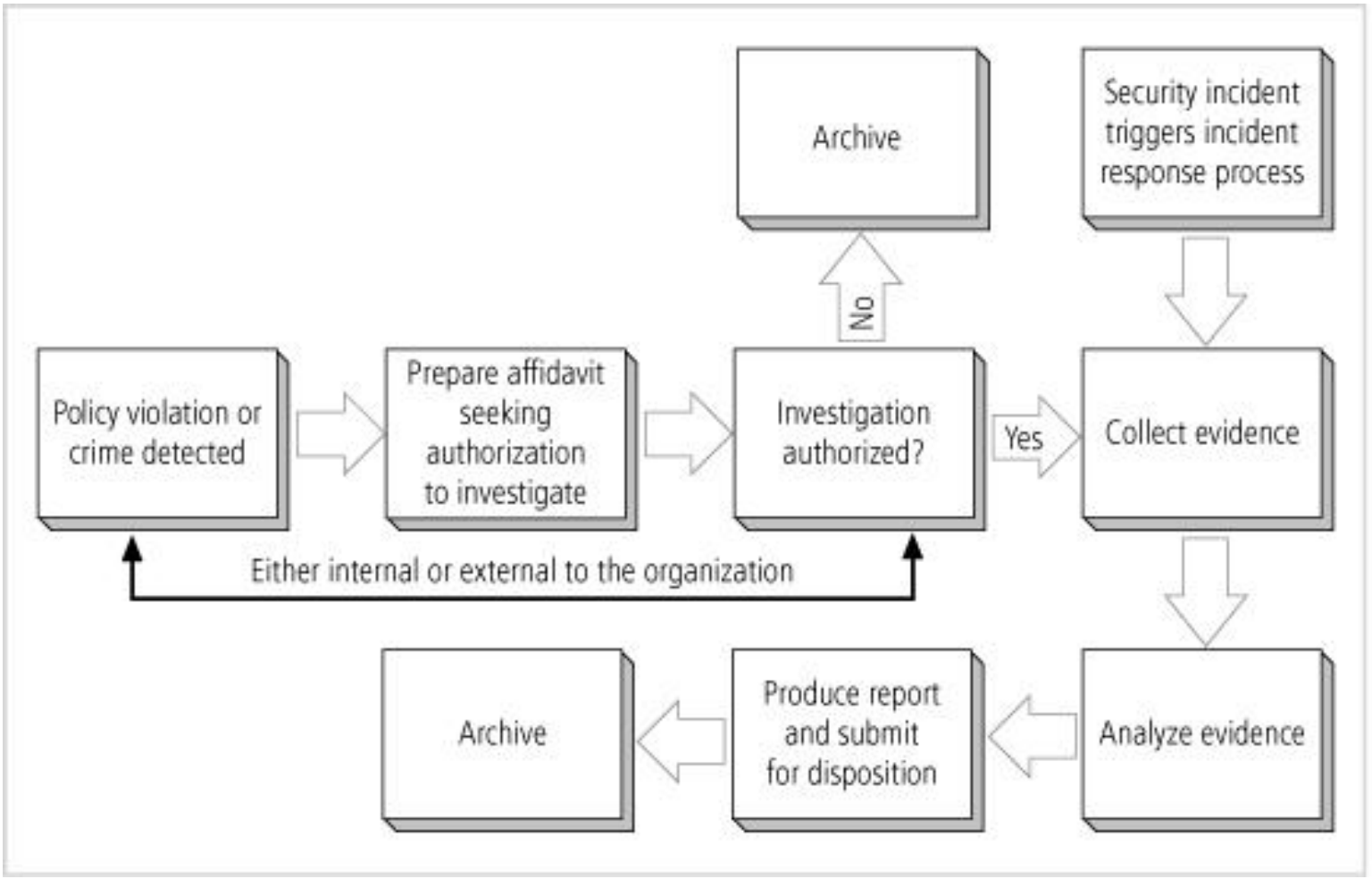
Managing Investigations

- **Digital forensics** can be used for two key purposes:
  - To investigate allegations of **digital malfeasance**
    - A crime against or using digital media, computer technology, or related components
  - To perform root cause analysis
    - Examine the path and methodology used in an incident
- Two approaches when employing digital forensics:
  - Protect and forget – patch and proceed
    - Focus on detection and analysis of events
  - Apprehend and prosecute – pursue and prosecute
    - Focus on identification of responsible individuals

Digital Forensics Team

- Most organizations cannot sustain a permanent digital forensics team
  - May be better to collect the data and then outsource the analysis component to a regional expert
- There should be people in the InfoSec group trained to understand and manage the forensics process
  - Expertise can be obtained by sending staff members to a regional or national InfoSec conference with a digital forensics track

Digital Forensics Process



Affidavits and Search Warrants

- **Affidavit**
  - Sworn testimony that certain facts are in the possession of the investigating officer
  - That the officer believes warrant the examination of specific items located at a specific place
- **Search warrant**
  - When an approving authority signs the affidavit or creates a synopsis form based on this document
  - Permission to search and seize items

Digital Forensics Methodology

- Identify relevant items of evidentiary value (EM)
- Acquire (seize) the evidence without alteration or damage
- Take steps to assure that the evidence is verifiably authentic and is unchanged
- Analyze the data without risking modification or unauthorized access
- Report the findings to the proper authority

Evidentiary Procedures

- In digital forensics, the focus is on procedures
- Organizations should develop specific procedures, along with guidance on the use of these procedures
- The policy document should specify:
  - Who may conduct the investigation
  - Who may authorize an investigation
  - What affidavit-related documents are required
  - What search warrant-related documents are required

Evidentiary Procedures

- The policy document should specify (cont'd):
  - What digital media may be seized or taken offline
  - What methodology should be followed
  - What methods are required for chain of custody or chain of evidence
  - What format the final report should take and to whom it should be given
- By creating and using these policies and procedures, an organization can best protect itself from challenges by employees who have been subject to unfavorable action resulting from an investigation