INFO 6027 W23

Week 12: Law, Privacy, and Ethics

FANSHAWE

Housekeeping

- Final exam is **Wednesday April 19th at 12:00 noon EST – Online!**
  - Registered part time or online students (or those studying abroad) are allowed to write at a different time, but you MUST email me.
  - Questions about the test (40% of final grade)
- **Questions about Assignment 3?**
- Please complete the **online student survey**! ☺

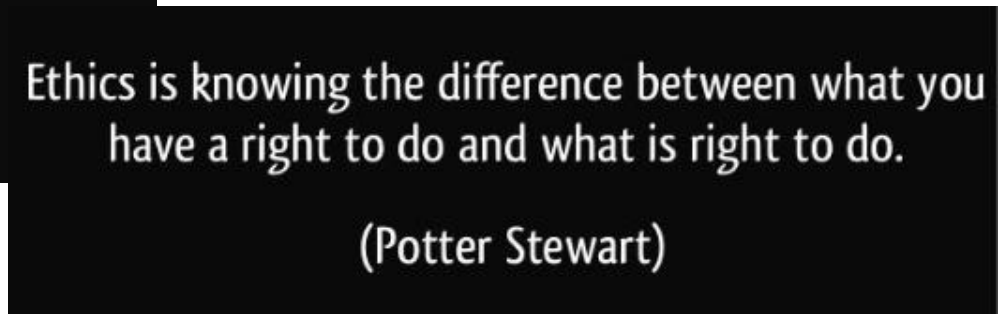
Agenda for this week

- Differentiate between **law** and **ethics**
- Describe the ethical foundations and approaches that underlie modern **codes of ethics**
- Identify key national and international laws that relate to the practice of information security
  - Canadian Laws
  - American (U.S.) Laws
- Describe the role of **culture** as it applies to ethics in information security
- Identify current information on laws, regulations, and relevant professional organizations

Guiding Questions

1. What is the difference between law, morals, and ethics, and how are they similar/connected?
2. Identify 5 different Canadian laws that relate to information security in some way. For each one, write a *brief* description of the purpose/scope
3. Why do you think we talk about privacy laws in this course?
4. Compare a piece of CDN legislation with its US counterpart. What differences do you notice?
5. What is the difference between policy and law?
6. Why are IT professionals prone to ethical issues?
7. What three conditions need to be met for deterrence to be effective?
8. What is organizational liability?
9. https://www.ted.com/talks/gaspard_koenig_do_we_really_own_our_bodies

Law and Ethics…



"In law a man is guilty when he violates the rights of others. In ethics he is guilty if he only thinks of doing so."

Immanuel Kant (1724 – 1804)

InfoSec Planning: Introduction to Law and Ethics

- All information security professionals must understand the scope of an organization's **legal** and **ethical** responsibilities
- Understand the *current* legal environment
  - Keep apprised of **new** laws, regulations, and ethical issues as they emerge (similar to how we begin our lectures)
  - To minimize the organization's **liabilities**
  - *Ignorance of the law is no excuse*
- Employees and management need to know their legal and ethical obligations
  - And proper use of information technology
  - Criminal (law) and civil law (liability)

  For Fun:

Law and Ethics in Information Security

- Laws
  - **Rules** adopted and enforced by **governments** to **codify** expected behavior in modern **society**
- The key difference between law and ethics is that law carries the **sanction** of a governing authority and ethics do not
- ***Ethics are based on cultural values*** (aka “mores”)
  - Relatively fixed moral attitudes or customs of a societal group
-

So….. Societal Morals/Values > Ethics > Laws

For Fun https://www.ted.com/talks/gaspard_koenig_do_we_really_own_our_bodies

Information Security and the Law

- InfoSec professionals and managers must understand the **legal framework** within which their organizations operate

This can influence the organization to a greater or lesser extent, depending on the nature of the organization and the scale on which it operates.

- For example, Some legal frameworks will force the organization to implement/institute certain things.
  - ex. COVID19 forcing the creation of laws that close businesses

For example, PIPEDA requires organizations to adopt physical, organizational and technological safeguards appropriate to the sensitivity of the personal information in question.

Types of Law

- Private law
  - Regulates the relationships among individuals and among individuals and organizations
    - Family law, commercial law, and labour law
- Public law
  - Regulates the structure and administration of government agencies and their relationships with citizens, employees, and other governments
    - Criminal, administrative, and constitutional law

Categories of Law

- Civil law
  - Pertains to relationships between and among **individuals and organizations**
- Criminal law
  - Addresses violations **harmful to society**
  - Actively enforced and prosecuted by the state
- Tort law
  - A subset of civil law that allows individuals to seek redress in the event of personal, physical, or financial **injury**

Privacy laws in Canada

FANSHAWE

Relevant Canadian Laws

- The Privacy Commissioner of Canada, is an officer of Parliament who reports directly to the House of Commons and the Senate.
- The Privacy Commissioner is an advocate for the privacy rights of Canadians. His (**Daniel Therrien's**) powers include:
  - Investigating complaints, conducting audits and pursuing court action under two federal laws;
  - Publicly reporting on the personal information-handling practices of public and private sector organizations;
  - Supporting, undertaking and publishing research into privacy issues; and
  - Promoting public awareness and understanding of privacy issues.

Determining what is private

Protected Information	Unprotected Information
Gender identification	Information that is not about an individual
Race / national / ethnic origin	Organizational information
Religion	Information that has been rendered anonymous (provided that it is not possible to link that data back to an identifiable person)
Age	Names of public servants
Marital status	Positions of public servants
Medical history	Titles of public servants
Education and employment history	Business contact information collected by an organization
Identifying numbers (e.g. SIN, drivers license)	Government information
Financial information	
DNA	

https://www.itworldcanada.com

Relevant Canadian Laws

- In Canada, your privacy rights are protected by **3 pieces of federal legislation:**
  1. *Privacy Act*
  2. *The Personal Information Protection and Electronic Documents Act* (PIPEDA).
  3. *Digital Privacy Act (2015)*

  There are also provincial privacy legislation
- Under these laws, individuals have the right to complain to the Privacy Commissioner of Canada about any alleged **mishandling of their personal information**.

- http://www.priv.gc.ca/index_e.cfm

PIPEDA

- Sets out ground rules for how **private sector organizations** may collect, use or disclose personal information in the course of **commercial activities**
- The law gives individuals the right to access and request correction of the personal information these organizations may have collected about them
- Became part of federal law in 2004
- In Ontario, applies to all organizations (except health industry, who are covered by PHIPA (2004)

Personal Information Protection and Electronic Document Act (PIPEDA) - 2004

- Accountability
- Identifying Purpose
- Consent
- Limited Collection
- Limited Use Disclosure & Retention
- Accuracy
- Safeguards
- Openness
- Individual Access
- Provide Recourse

Other Relevant Canadian Laws

- **Most cyber crime falls under the Criminal Code of Canada**
  - **http://laws.justice.gc.ca/eng/C-46/index.html**
- **Bill C-11: Copyright Modernization Act (2012)** updates 1997 Copyright laws to include Digital Copyright & Digital Locks
- http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=5697419

- **Security of Information Act (1985)**
- There is also CASL (Canadian Anti-Spam Law) from 2010
- Bill C-59 (National Security laws)

- And many more….

Relevant Canadian Laws

Criminal Code (R.S.C., 1985, c. C-46)
Full Document: HTML (Accessibility Buttons available) | XML [4776 KB] | PDF [7237 KB]
Act current to 2020-11-17 and last amended on 2020-07-01. Previous Versions

Criminal harassment

264 (1) No person shall, without lawful authority and knowing that another person is harassed or recklessly as to whether the other person is harassed, engage in conduct referred to in subsection (2) that causes that other person reasonably, in all the circumstances, to fear for their safety or the safety of anyone known to them.

Prohibited conduct

(2) The conduct mentioned in subsection (1) consists of

(a) repeatedly following from place to place the other person or anyone known to them;

(b) repeatedly communicating with, either directly or indirectly, the other person or anyone known to them;

(c) besetting or watching the dwelling-house, or place where the other person, or anyone known to them, resides, works, carries on business or happens to be; or

(d) engaging in threatening conduct directed at the other person or any member of their family.

Punishment

Relevant Canadian Privacy Laws

- Each province has provincial privacy laws
- In Ontario, government organizations are covered by Office of the Chief Information and Privacy Officer & FIPPA: **Freedom of Information and Protection of Privacy Act**
  - https://www.ontario.ca/laws/statute/90f31
- MFIPPA: Municipal FIPPA
  - http://www.london.ca/city-hall/mfippa/Pages/MFIPPA.aspx
- PHIPA: Personal Health Information and Protection Act
  - http://www.ontario.ca/laws/statute/04p03
- FOIRA: Freedom of Information Request http://www.accessandprivacy.gov.on.ca/

Relevant U.S. Laws

FANSHAWE

Relevant U.S. Laws

- The Computer Fraud and Abuse Act of 1986 (CFA Act)
  - The cornerstone of many computer-related federal laws and enforcement efforts
  - Amended in October 1996 by the National Information Infrastructure Protection Act
    - Modified several sections of the previous act, and increased the penalties for select crimes
  - Further modified by the USA PATRIOT Act of 2001, re2006
    - Provides law enforcement agencies with broader latitude to combat terrorism-related activities
    - The USA PATRIOT Act was updated and extended, in many cases permanently
      - Through the USA PATRIOT Improvement and Reauthorization Act of 2005

Relevant U.S. Laws

The Computer Security Act of 1987

- One of the first attempts to protect federal computer systems
  - Established minimum acceptable security practices

- Established a Computer System Security and Privacy Advisory
  - Board within the **Department of Commerce**

- Requires ***mandatory periodic training in computer security awareness*** and accepted computer security practice ***for all users of Federal computer systems***

- Charged the National Bureau of Standards (**became NIST in 1988**) and the NSA with the development of multiple standards and guidelines.

Relevant U.S. Laws

- Privacy Laws
  - –Many organizations collect, trade, and sell ***personal information as a commodity***
    - Individuals are becoming aware of these practices and **looking to governments to protect their privacy**
  - –Aggregation of data from multiple sources permits unethical organizations to build databases with alarming quantities of personal information
  - –The **Privacy of Customer Information** section of regulations covering common telecommunications carriers
    - Specifies that any proprietary information shall be used explicitly for providing services, and not for any marketing purposes
    - https://www.law.cornell.edu/uscode/text/47/222

Relevant U.S. Laws

- Privacy Laws (cont'd)
  - **The Federal Privacy Act** of 1974 regulates the government's use of private information
    - Ensure that government agencies protect the privacy of individuals' and businesses' information
  - **The Electronic Communications Privacy Act** of 1986
    - A collection of statutes that regulates the interception of wire, electronic, and oral communications

These statutes work in cooperation with the **Fourth Amendment** of the U.S. Constitution

- Prohibits search and seizure without a warrant

Relevant U.S. Laws

- Health Insurance Portability & Accountability Act Of 1996 (HIPAA)
  - –An attempt to protect the confidentiality and security of health care data
    - Establishes and enforces standards
    - Standardizes electronic data interchange
  - –Requires organizations that retain health care information to use information security mechanisms to protect this information
    - Also requires an assessment of the organization's InfoSec systems, policies, and procedures

What does HIPPA have to do with infosec?

Relevant U.S. Laws

- The Financial Services Modernization Act
  - –Also called **G**ramm-**L**each-**B**liley Act of 1999
  - –Applies to financial institutions (ie banks, securities firms, and insurance companies)
  - –Requires all financial institutions to **disclose their privacy policies**
    - Describing how they share nonpublic personal information
    - Describing how customers can request that their information not be shared with third parties
  - –Ensures that the privacy policies in effect in an organization are fully disclosed when a customer initiates a business relationship
    - Distributed at least annually for the duration of the professional association

Relevant U.S. Laws

- Export and Espionage Laws
  - **Economic Espionage Act (EEA) of 1996**
    - An attempt to **protect intellectual property** and **competitive advantage**
    - Attempts to protect **trade secrets** from the foreign government that uses its classic espionage apparatus to spy on a company
      - Also between two companies
      - Or a disgruntled former employee
    - https://www.law.cornell.edu/uscode/text/18/1831

Relevant U.S. Laws

- Export and Espionage Laws
  - –The **Security and Freedom through Encryption (SAFE) Act** of 1997
    - Provides guidance on the use of encryption
    - Institutes measures of public protection from government intervention
    - ***Reinforces an individual's right to use or sell encryption algorithms***
    - Prohibits the federal government from requiring the use of encryption for contracts, keys, grants, and other official documents, and correspondence
    - http://csrc.nist.gov/nissc/1998/proceedings/paperG5.pdf

- *"Denying millions of law-abiding people the use of a legitimate and increasingly necessary security product for 'law enforcement reasons' is like banning deadbolt locks because they make it a little harder to kick down the doors of a few drug dealers."*

U.S Senator Conrad Burns

Relevant U.S. Laws

- U.S. Copyright Law
  - Extends protection to intellectual property, including words published in electronic formats
  - 'Fair use' allows material to be quoted so long as ***the purpose is educational and not for profit, and the usage is not excessive***
  - Proper acknowledgement must be provided to the author and/or copyright holder of such works
    - Including a description of the location of source materials, using a recognized form of citation
- Digital Millennium Copyright Act -1998
  - Codifies (makes law) the WIPO treaties of 1996, (EU)
    - protection of works and the rights of their authors in the digital environment
    - World Intellectual Property Organization

Relevant U.S. Laws

- Freedom of Information Act of 1966
  - –All Federal agencies are required to disclose records requested in writing by any person
  - –Applies only to Federal agencies and does not create a right of access to records held by Congress, the courts, or by state or local government agencies

Relevant U.S. Laws

- **Sarbanes-Oxley Act of 2002**
  - Prompted by the **Enron scandal**
  - Enforces accountability for the *financial record keeping and reporting* at publicly traded corporations
  - Requires that the CEO and chief financial officer (CFO) ***assume direct and personal accountability*** for the completeness and accuracy of a publicly traded organization's financial reporting and record-keeping systems
    - As these executives attempt to ensure that the systems used to record and report are sound, ***the related areas of availability and confidentiality are also emphasized***

International Laws and Legal Bodies

- International trade is governed by international treaties and trade agreements
  - –Many domestic laws and customs do not apply
  - –Laws in the US, or Canada, may not be law in other countries
- There are currently **only a few** international laws relating to privacy and information security
  - –Because of cultural differences and political complexities of the relationships among nations

International Laws and Legal Bodies

- European Council Cyber-Crime Convention (2004)
  - –Empowers an international task force to oversee a range of Internet security functions
    - Attempts to resolve the issue of JURISDICTION
    - Includes Internet Investigations
    - Standardizes technology laws internationally
  - –Attempts to improve the effectiveness of international investigations into breaches of technology law
  - –Goal is to simplify the acquisition of information for law enforcement agents in certain types of international crimes, as well as the extradition process

International Laws and Legal Bodies

- The Digital Millennium Copyright Act (DMCA) 1998
  - –A U.S.-based international effort to reduce the impact of copyright, trademark, and privacy infringement, especially via the removal of technological copyright protection measures, aka *Digital Rights Management (DRM)*
  - –Born from the WIPO treaties of 1996
  - - Protects copyrighted material in digital format
- **European Data Protection Directive** (95/46/EC)
  - –Increases individual rights to process/freely move personal data
- "**Database right**" is the U.K. version of this directive
- **GDPR** – General Data Protection Regulations

Policy Versus Law

- Difference between policy and law
  - –Ignorance of policy may be an acceptable defense, not in law, however
- Policies must be:
  1. **Distributed** to all individuals who are expected to comply with them
  2. Easily read and understood, with multilingual, visually impaired and low- literacy translations (can be read by everyone – accessible)
  3. Readily available for employee reference
  4. Acknowledged by employee with consent form (compliance)
  5. Uniformly enforced for all employees (regardless of status/rank)

Ethics in Information Security

FANSHAWE

Ethics in Information Security

Information security students are not expected to study the topic of **ethics in a vacuum**, but within a larger ethical framework

- Information security professionals may be expected to be more articulate about the topic than others in the organization
  - **Often subject to a higher degree of scrutiny**
- Is it ok to read people's emails if you are looking for phishing attempts? Or to look at pictures if searching for pornography? Documents? Web traffic? *IT Professionals have a lot of access to private information*.

Examples of ethical issues:

- Your boss tells you to ignore a legislated security requirement because of the cost to implement.
- Your co-worker invites you to a party, and you pick which dish to bring based on your review of that person's internet activity.
- Your access to information allows you to know a job posting before your peers.
- You learn of a child who has been abducted near your organization. Several co-workers want you to send an email to everyone asking employees to share anything they saw that might help.
- You hear that your department may be cutting infosec jobs because there haven't been any security breaches in 3 years. You are worried you may be fired. Do you *accidentally* create a vulnerability?
- Any other ideas?

The 10 Directives of Computer Ethics

You must:

1. **Not Use a computer to harm other people**
2. **Not Interfere with other people's computer work**
3. **Not Snoop around in other people's computer files**
4. **Not Use a computer to steal**
5. **Not Use a computer to bear false witness**
6. **Not Copy or use proprietary software for which you have not paid**
7. **Not Use other people's computer resources without authorization or proper compensation**
8. **Not Appropriate other people's intellectual output**
9. **Think about the social consequences of the program you are writing or the system you are designing**
10. **Always use a computer in ways that ensure consideration and respect for your fellow humans**

Ethics and Education

- Differences in *computer use ethics* are not exclusively cultural. Differences can be found among individuals within the same country, within the same social class, and within the same company

- Key studies reveal that the overriding factor in leveling the ethical perceptions within a small population is **education**

- Employees must be trained on the expected behaviors of an ethical employee

Deterring Unethical and Illegal Behavior

- **Deterrence** is the best method for preventing an illegal or unethical activity
- Laws, policies, and technical controls are all examples of deterrents
- However, it is generally agreed that laws and policies and their associated penalties **only deter if three conditions are present**
  1. Fear of penalty
  2. Probability of being caught
  3. Probability of consequence (penalty) being administered

Professional Orgs and their Codes of Ethics

- Some professional organizations have established **codes of conduct** and/or codes of ethics
  - –Members are expected to follow
  - –Codes of ethics can have a positive effect on an individual's judgment regarding computer use
- Security professionals must act ethically
  - –According to the policies and procedures of their employers, their professional organizations, and the laws of society.
  - – **Certifications can be stripped** from individuals in violation

Professional Organization	Web Resource Location	Description	Focus
Association of Computing Machinery	*www.acm.org*	Code of 24 imperatives of personal ethical responsibilities of security professionals	Ethics of security professionals
Information Systems Audit and Control Association	*www.isaca.org*	One process area and six subject areas that focus on auditing, information security, business process analysis, and IS planning through the CISA and CISM certifications	Tasks and knowledge required of the information systems audit professional
Information Systems Security Association	*www.issa.org*	Professional association of information systems security professionals; provides education forums, publications, and peer networking for members	Professional security information sharing
International Information Systems Security Certification Consortium $(ISC)^2$	*www.isc2.org*	International Consortium dedicated to improving the quality of security professionals through SSCP and CISSP certifications	Requires certificants to follow its published code of ethics
SANS Institutes Global Information Assurance Certification	*www.giac.org*	GIAC certifications focus on four security areas: security administration, security management, IT audit, and software security, and has standard, gold, and expert levels	Requires certificants to follow its published code of ethics

International Information Systems Security Certification Consortium, Inc.

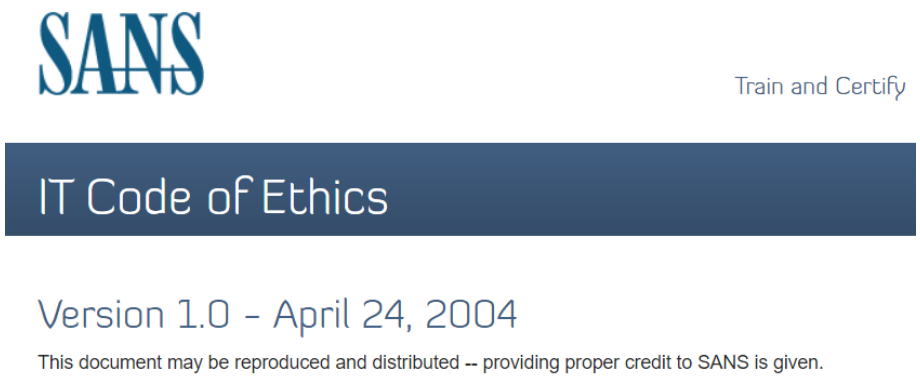
(ISC)²

- Code of ethics applies to information security professionals who have earned one of their certifications
  - Includes four mandatory canons:
    1. Protect society, the commonwealth, and the infrastructure
    2. Act honorably, honestly, justly, responsibly, and legally
    3. Provide diligent and competent service to principals
    4. Advance and protect the profession

    https://www.isc2.org/Ethics#

System Administration, Networking, and Security (SANS) Institute

- Professional research and education cooperative organization
  - –Over 165,000 security professionals, auditors, system and network administrators around the world
- SANS **GIAC** code of ethics requires:
  - –Respect for the public
  - –Respect for the certification
  - –Respect for my employer
  - –Respect for myself



Information Systems Security Association (ISSA)

- Nonprofit society of information security professionals
- Mission is **to bring together qualified practitioners of information security for information exchange and educational development**
- Provides conferences, meetings, publications, and information resources to promote information security awareness and education
- Promotes a code of ethics
  - Similar to that of other organizations
  - ***"Promoting management practices that will ensure the confidentiality, integrity, and availability of organizational information resources."***

https://www.issa.org/issa-code-of-ethics/

Information Systems Audit and Control Association (ISACA)

- Serves 140,000 professionals in 180 countries
- A professional association with a focus on auditing, control, and security
- Membership comprises both technical and managerial professionals
- Has a code of ethics for its professionals
- Requires many of the same high standards for ethical performance as the other organizations and certifications

https://www.isaca.org/credentialing/code-of-professional-ethics

ISACA code of Ethics has 7 Tenets

- Code of ethics tenets. **Members shall:**
  1. Support the implementation of, and encourage compliance with, appropriate standards, procedures, and information systems controls
  2. Perform duties with objectivity, due diligence and professional care, using professional standards and best practices
  3. Serve in the interest of stakeholders in a lawful and honest manner, maintain high standards of conduct and character, and not engage in acts discreditable to the profession
  4. Maintain the privacy and confidentiality of information obtained in the course of their duties
     - Unless disclosure is required by legal authority
     - Such information shall not be used for personal benefit or released to inappropriate parties

Information Systems Audit and Control Association

5. Maintain competency in their respective fields, and agree to undertake only those activities that they can reasonably expect to complete with professional competence
6. Inform appropriate parties of the results of work performed, revealing all significant facts known to them
7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control

Canadian Information Processing Society (CIPS)

- All CIPS members (including students) agree to abide by the Code of Ethics and its ethical principles/imperatives:
  - Protecting the Public Interest and Maintaining Integrity;
  - Demonstrating Competence and Quality of Service;
  - Maintaining Confidential Information and Privacy;
  - Avoiding Conflict of Interest; and
  - Upholding Responsibility to the IT Profession.
- Code of Ethics and Professional Conduct (New!) (.pdf)

- **Discipline and Enforcement (for international members only. Members residing in Canada need to visit their respective Provincial Association website - http://www.cips.ca/Provinces)**
  - Enforcement Process, Hearing Process, Ethical Principles, etc.

Organizational Liability and the Need for Counsel

- What if an organization does not support or encourage strong ethical conduct by its employees?
- What if an organization does not behave ethically?
- If an employee, acting with or without the authorization, performs an illegal or unethical act, causing some degree of harm, **the organization can be held financially liable** for that action

Organizational Liability and the Need for Counsel

- An organization increases its liability if it refuses to take measures ("**due care**" or "should have done") to make sure that every employee knows what is acceptable and what is not, and the consequences of illegal or unethical actions
- **Due diligence** (facts and decisions) requires that an organization make a valid and ongoing effort to protect others

CDN Law Enforcement Agencies

- RCMP Technical Crimes division
  - Deal with Interpol and various US law enforcement agencies
  - Deal with national issues
  - Canadian Anti-Fraud Center
- OPP Technical Crimes division
  - Provincial crime enforcement
  - Child pornography division as well
- Local Law enforcement Technical divisions
  - Local crimes - London Police Service has 2 full-time officers.
- All divisions are cooperative amongst each other

LPS/RCMP Inter-agency collaboration

Internal Investigations

FANSHAWE

Managing Investigations in the Organization

- When (not if) an organization finds itself dealing with a suspected policy or law violation
  - **Must appoint an individual to investigate it**
  - How the internal investigation proceeds
    - Dictates whether or not the organization has the ability to take action against the perpetrator if in fact evidence is found that substantiates the charge

- In order to protect the organization, and to possibly assist law enforcement in the conduct of an investigation
  - The investigator (CISO, InfoSec Manager or other appointed individual) must document what happened and how

Managing Investigations in the Organization

- Forensics
  - The coherent application of methodical investigatory techniques to present evidence of crimes in a court or court-like setting
- Digital forensics
  - The investigation of what happened and how
  - Involves the preservation, identification, extraction, documentation, and interpretation of computer media for evidentiary and/or root cause analysis
  - Like traditional forensics, it follows clear, well-defined methodologies, but still tends to be as much art as science

Managing Investigations in the Organization

- Digital forensics can be used for two key purposes:
  - Investigate allegations of digital malfeasance
    - A crime against or using digital media, computer technology or related components
  - Perform root cause analysis
    - If an incident occurs and the organization suspects an attack was successful, digital forensics can be used to examine the path and methodology used to gain unauthorized access, as well as to determine how pervasive and successful the attack was

Managing Investigations in the Organization

- Digital forensics approaches
  - –Protect and forget (a.k.a. patch and proceed)
    - Focuses on the defense of the data and the systems that house, use, and transmit it
  - –Apprehend and prosecute (a.k.a. pursue and prosecute)
    - Focuses on the identification and apprehension of responsible individuals, with additional attention on the collection and preservation of potential EM that might support administrative or criminal prosecution

Managing Investigations in the Organization

- Evidentiary material (EM)
  - –Also called item of potential evidentiary value
  - –Any information that could potentially support the organization's legal-based or policy-based case against a suspect
  - –An item does not become evidence until it is formally admitted to evidence by a judge or other ruling official

Affidavits and Search Warrants

- Investigations begin with an allegation or an indication of an incident
- Forensics team requests permission to examine digital media for potential Evidentiary Material (EM)
- An “affidavit” is a sworn testimony
  - That the investigating officer has certain facts they feel warrant the examination of specific items located at a specific place

Affidavits and Search Warrants

- Search warrant
  - –Judicial permission to search for EM at the specified location and/or to seize items to return to the investigator’s lab for examination
  - –Created when an approving authority signs the affidavit or creates a synopsis form based on it

Evidentiary Procedures

- Organizations should develop specific procedures and guidance for their use (cont'd.)
  - 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 it be given

Summary

- Introduction
- Law and ethics in information security
- The legal environment
- Ethical concepts in information security
- Professional organizations' codes of ethics
- Organizational liability and the need for counsel
- Key CDN & USA agencies
- Managing investigations in the organization

References and Reminders

- **Computer Security Principles and Practice**. 4th Ed. (Stallings & Brown, 2018)
- **Principles of information Security**. 6th Ed. (Whitman & Mattord, 2018)
- Other links as posted in presentation slides

Reminders:

- Assignment 3 is due August 07

Next week we will discuss:

- Physical Security

Review for Final Test

Find an online tool for creating flashcards. Options include:

- Cram.com (nice one for sharing with your peers…)
- StudyBlue
- Brainscape
- Flashdecks
- Quizet.com
- Anki

Using the lesson content (textbook, slides, lecture audio, notes, articles, discussion forums, labs, etc.), create a set of flashcards.

Test Preparation Exercise:

Once you complete your flashcards, share them with your study group members. Set a time to "meet" online and go over the cards as a group. Edit them and take notes. You can even turn it into a game to see who can "stump" the group with their cards!


Thank You