ACS-2821-001

Information Security in Business

Law, Investigations, and Ethics

ACS-2821-001 – Slides Used In The Course

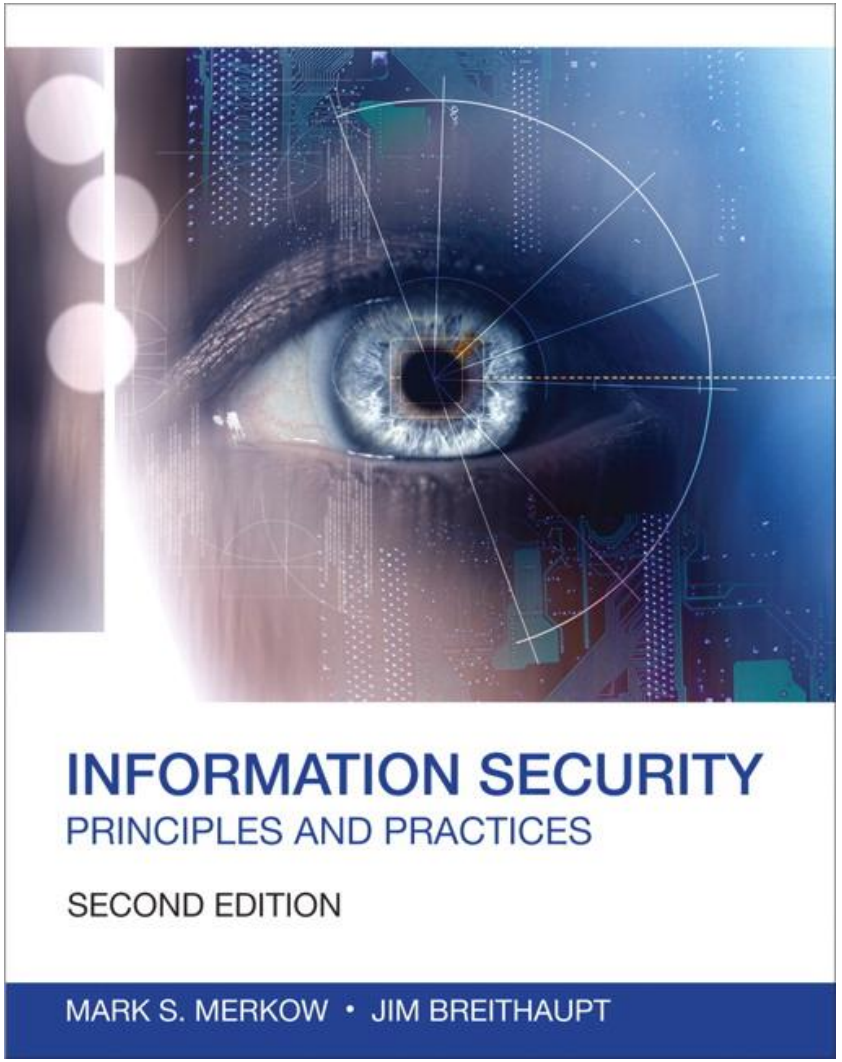
THE UNIVERSITY OF WINNIPEG

A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.



Objectives

- Identify the types and targets of computer crime
- Summarize the major types of attacks performed by cyber criminals
- Understand the context of the computer in the legal system
- Appreciate the complexities of intellectual property law
- Discuss the issues surrounding computer security and privacy rights
- Articulate the challenges of computer forensics
- Recognize ethical issues related to information security

Overview

- IS specialists need to keep up with the latest laws, codes of ethics, and other rules governing the use of information technology
- The speed of technological change outstrips the speed at which our governing bodies can create applicable laws
- This gap makes the IS specialist's role even more critical

Types of Computer Crime

- The 2013 Verizon Data Breach Investigations report revealed that
  - More than 47,000 security incidents were reported
  - 75% of attacks are driven by financial motives
  - 71% of attacks targeted user devices and 54% compromised servers
  - 69% of attacks were discovered by external parties
  - 66% attacks took months of longer to discover

Types of Computer Crime

- Major categories of computer crimes
  - Military and intelligence attacks
  - Business attacks
  - Financial attacks
  - Terrorist attacks
  - Grudge attacks
  - Thrill attacks

Types of Computer Crime

THE UNIVERSITY OF WINNIPEG

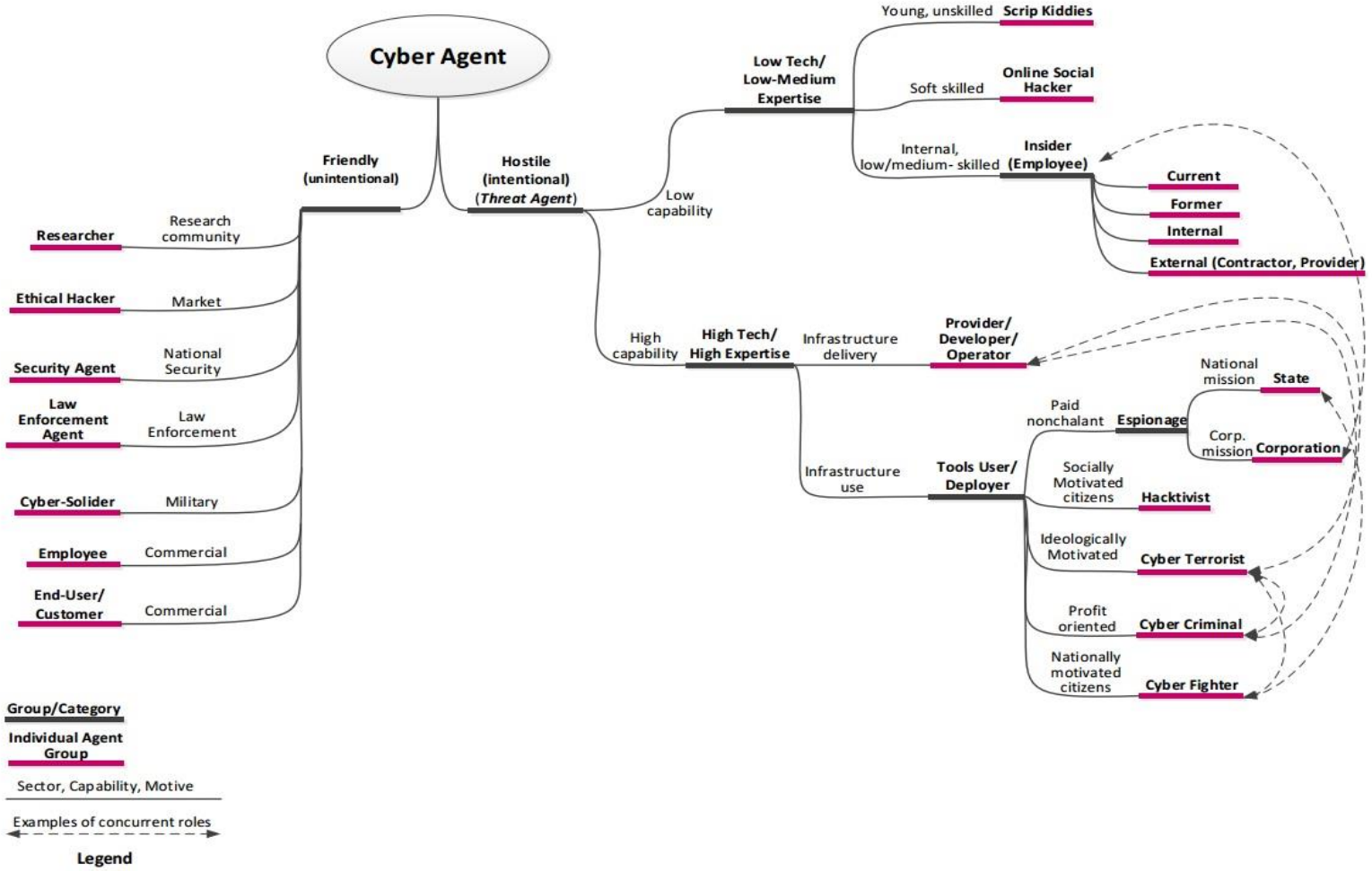
Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⊃	1. Malware	⊃	→
2. Web Based Attacks	∩	2. Web Based Attacks	∩	→
3. Web Application Attacks	∩	3. Web Application Attacks	⊃	→
4. Phishing	∩	4. Phishing	∩	→
5. Spam	∩	5. Denial of Service	∩	↑
6. Denial of Service	∩	6. Spam	⊃	↓
7. Ransomware	∩	7. Botnets	∩	↑
8. Botnets	∩	8. Data Breaches	∩	↑
9. Insider threat	⊃	9. Insider Threat	∪	→
10. Physical manipulation/ damage/ theft/loss	⊃	10. Physical manipulation/ damage/ theft/loss	⊃	→
11. Data Breaches	∩	11. Information Leakage	∩	↑
12. Identity Theft	∩	12. Identity Theft	∩	→
13. Information Leakage	∩	13. Cryptojacking	∩	NEW
14. Exploit Kits	∪	14. Ransomware	∪	↓
15. Cyber Espionage	∩	15. Cyber Espionage	∪	→

Legend: Trends: ∪ Declining, ⊃ Stable, ∩ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Table 4 - Overview and comparison of the current threat landscape 2018 with the one of 2017

Source: ENISA Threat Landscape Report 2018

Types of Hackers



Source: Marinos, Louis, A. Belmonte, E. Rekleitis, "ENISA Threat Landscape 2015," ENISA, January 2016, Greece

Types of Hackers

THE UNIVERSITY OF WINNIPEG

- **White Hat**
  - Computer experts who specialise in testing systems
  - Help to find and point out flaws
  - Provide service like penetration test in order to help companies
- **Black Hat**
  - The bad guys who break into computers or networks or create viruses to steal information and take control
  - Their aim is to profit from selling their services or the information they steal.
- **Grey Hat**
  - They test and exploit weaknesses in systems without the knowledge or permission of their targets
  - Grey hat hackers will, however, reveal the flaws they find to their victims in exchange for being paid.
- **Script Kiddies**
  - Young and inexperienced hackers who use off the shelf programs to attack networks and interfere with websites in order to try to make their name.

Types of Hackers

- **Hacktivists**
  - Hackers with political or ideological motivations
  - They perform attacks to expose what they perceive as wrongdoing or to exact revenge against groups or companies that they believe are behaving immorally.
- **State Sponsored**
  - Supported by and doing the work of governments
  - They have an armies of cyber warriors who attack institutions in their government's interests.
- **Corporate Sponsored**
  - Hackers who are hired to break into the competition and steal valuable trade secrets
  - They are paid by a company or a middle man to perform specific attacks.
- **Cyber Terrorists**
  - Hackers who are religiously or ideologically motivated
  - Their aim is to spread fear and create chaos by attacking institutions and causing unrest.

How Cyber Criminals Commit Crimes

- Most prevalent types of computer crimes
  - Denial-of-Service (DoS) attacks
  - Rogue code
  - Software piracy
  - Social engineering
  - Dumpster diving
  - Spoofing of Internet Protocol addresses
  - Emanation eavesdropping
  - Embezzlement
  - Information warfare

The Computer and the Law

- Three branches of the legal system
  - Legislative branch (Congress and Senate for the US, House of Common and House of Senate for Canada))
    - Statuary law, referred to as session law
  - Administrative branch
    - Administrative law, also referred to as natural justice
    - Disputes are resolved before an administrative tribunal, not a court
  - Judicial branch
    - Common law

The Computer and the Law

- Three primary categories in common law
  - Civil law: Compensates individuals who were harmed through wrongful acts known as torts
    - Does not involve imprisonment only fines
  - Criminal law: Punishes those who violate government laws and harm an individual or group
    - Involves imprisonment in addition to fines
  - Regulatory law: Regulates the behavior of administrative agencies of government
    - Can exact both financial penalties and imprisonment

Intellectual Property Law

- Besides copyright protection, designed to protect the distribution and reproduction rights of the owner, intellectual property law includes several other categories:
  - Patent law
    - Patents grant an inventor the right to exclude others from producing or using the inventor's discovery or invention for a limited period of time
    - Patents are good for 17 years in the USA, for Canada patents are good for 20 years
    - Patents are given to software

Intellectual Property Law

- Besides copyright protection, designed to protect the distribution and reproduction rights of the owner, intellectual property law includes several other categories:
  - Trademarks
    - Trademarks are any word, name, symbol, or device, or any combination thereof that the individual intends to use commercially and wants to distinguish as coming from a unique source
  - Trade secrets
    - A trade secret is a patent in process, an embryonic but unofficial and legally unprotected idea

Intellectual Property Law

- Fair Information Practices in the Electronic Marketplace (source: the Federal Trade Commission's May 2000 report)
  - Notice/awareness
    - Web site should tell the user how it collects and handles user information
  - Choice/consent
    - Web sites must give consumers control over how their personally identifying information is used

Privacy and the Law

- Fair Information Practices in the Electronic Marketplace (source: the Federal Trade Commission's May 2000 report)
  - Access/participation
    - Users would be able to review, correct, and in some cases delete personally identifying information on a particular Web site
  - Security/integrity
    - Web sites must implement policies, procedures, and tools that will prevent unauthorized access and hostile attacks against the site

International Privacy Issues

- The International Safe Harbor Principles
  - Notice
    - Companies must notify individuals what personally identifying information they are collecting, why they are collecting it, and how to contact the collectors
  - Choice
    - Individuals must choose whether and how their personal information is used by, or disclosed to, third parties
  - Onward transfer
    - Third parties receiving personal information must provide the same level of privacy protection as the company from whom the information is obtained

International Privacy Issues

- The International Safe Harbor Principles
  - Security
    - Companies housing personal information and sensitive data must secure the data
  - Data integrity
    - Companies must reassure individuals that their data is complete, accurate, current, and used for the stated purposes only
  - Access
    - Individuals must have the right and ability to access their information and correct, modify, or delete any portion of it

International Privacy Issues

- The International Safe Harbor Principles
  - Enforcement
    - Each company must adopt policies and practices that enforce the aforementioned privacy principles

Privacy Laws in the United States

THE UNIVERSITY OF WINNIPEG

- 1970 **U.S. Fair Credit Reporting Act**: Regulates the activities of credit bureaus
- 1986 **U.S. Electronic Communications Act**: Protects the confidentiality of private message systems through unauthorized eavesdropping
- 1987 **U.S. Computer Security Act**: Improves the security and privacy of sensitive information in federal computer systems
- 1996 **U.S. Kennedy-Kassenbaum Health Insurance and Portability Accountability Act (HIPAA)**: Protects the confidentiality and portability of personal health care information

Privacy Laws in the United States

- 2000 **National Security Directive 42 (NSD-42)**: Gives guidance on the security of national defense systems, among other roles
- 2001 **U.S. Patriot Act HR 3162**, aka "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act"
- 2002 **Federal Information Security Management Act**: Defines the basic statutory requirements for protecting federal computer systems
- 2010 **Fair Depth Collection Practices Act**: Addresses unfair or unconscionable means to collect or attempt to collect a debt

Privacy Laws in the Canada

The Office of the Privacy Commissioner of Canada (OPC) oversees compliance with two federal privacy laws:

- **The Privacy Act**
  - Covers the personal information-handling practices of federal government departments and agencies.
- **The Personal Information Protection and Electronic Documents Act (PIPEDA)**
  - Covers the personal information-handling practices of many businesses.

Each provinces and territories also has there own sets of privacy legislation

Computer Forensics

- The National Data Conversion Institute (NDCI) makes a case for using expert investigative services to solve computer crimes
- Arguments for the advantages of using investigative services
  - Successful litigation frequently depends on obtaining irrefutable computer evidence
  - Your evidence may not be as good as the opposition's if you are using less sophisticated data-detection techniques
  - Your adversaries do not want you to obtain the data you need
  - The technology used to create the data you need may have already disappeared. Time is of the essence.

The Information Security Professional's Code of Ethics

- ISC^2 Code of Ethics: Four mandatory code
  - 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

The Information Security Professional's Code of Ethics

THE UNIVERSITY OF WINNIPEG

- ISACA Code of Ethics:
  - Support the implementation of, and encourage compliance with, appropriate standards and procedures for the effective governance and management of enterprise information systems and technology, including: audit, control, security and risk management.
  - Perform their duties with objectivity, due diligence and professional care, in accordance with professional standards.
  - Serve in the interest of stakeholders in a lawful manner, while maintaining high tandards of conduct and character, and not discrediting their profession or the Association.
  - Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
  - Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.
  - Inform appropriate parties of the results of work performed including the disclosure of all significant facts known to them that, if not disclosed, may distort the reporting of the results.
  - Support the professional education of stakeholders in enhancing their understanding of the governance and management of enterprise information systems and technology, including: audit, control, security and risk management.

Other Ethics Standards

- Computer Ethics Institute's Ten Commandments of Computer Ethics
- Internet Activities Board's Ethics and the Internet
- U.S. Department of Health, Education, and Welfare - Code of Fair Information Practices

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.

Summary

- Laws, investigative principles, and professional ethics are as important to information security professionals as knowing how to design firewall architecture, which is a fundamental security technology

ACS-2821-001 – Questions?