



Lesson 15 – Regulations, Standards, Legal, Ethical, & Professional Issues



"You know, you can do this just as easily online."

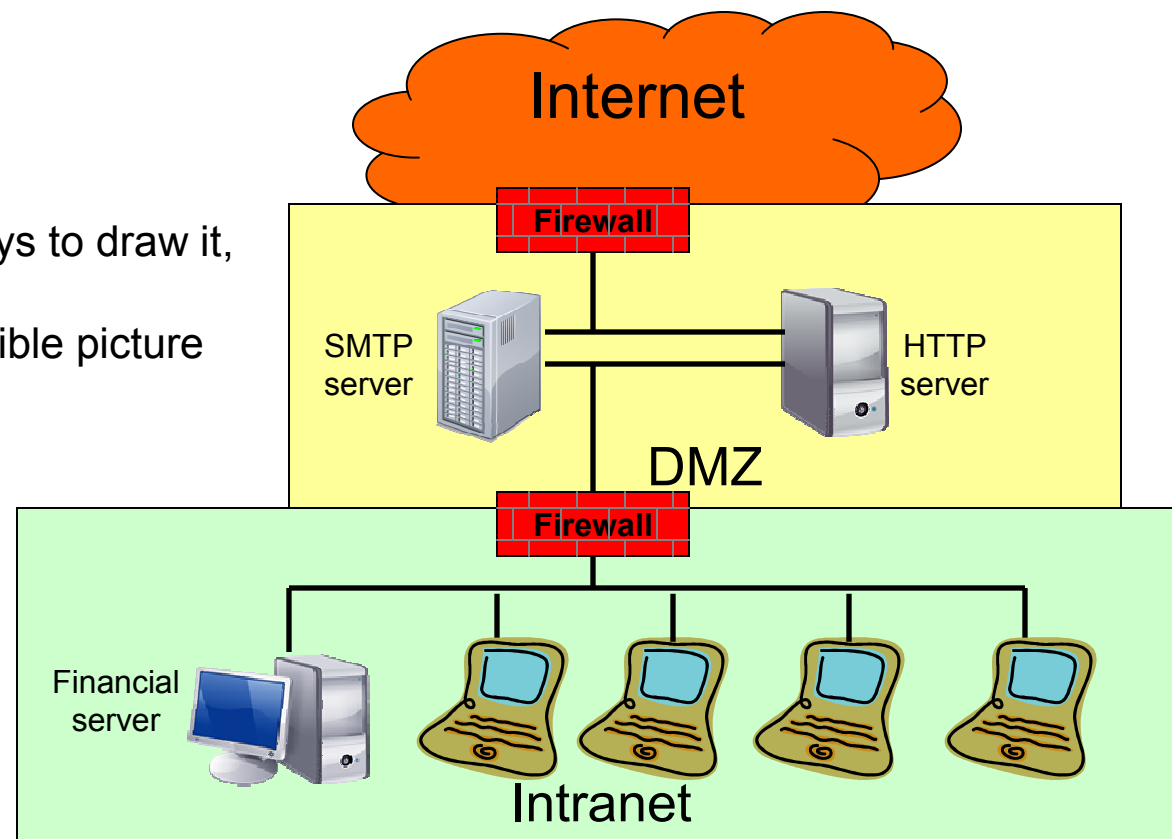
Quiz review

- Imagine that, you are working on a small company that has the following hardware: four Personal Computers (PCs), one email server (SMTP), one web server (HTTP), one internal server with sensitive financial information, and two hardware firewalls (for a total of nine machines). All the machines are in a network that is connected with the Internet, but management wants to implement a DMZ
- Note:
 - Exposed to the Internet (and so, must be in DMZ)
 - 1 SMTP server
 - 1 HTTP server
 - Containing sensitive company data (must be in the intranet)
 - 1 Internal server with sensitive financial information
 - 4 PCs
 - 2 Firewalls

Quiz

- Draw a picture of a network for the small company that implements a DMZ configuration

There are multiple ways to draw it,
and so,
this is just one possible picture



Quiz

- What is an asset?
 - Asset is a resource, process, product, or system that has value to the organization
 - Type of assets
 - Tangible
 - Examples: computer hardware, computer data, licensed products, and software applications
 - Intangible.
 - Examples: data privacy and the organization's public image
- What is a security policy? How is a security policy used?
 - A formal set of rules regarding an organization's technology and information assets, which users must follow
 - A security policy combines the policies required by senior management with any regulatory policy requirements

Quiz

Question 3: What is an exploit? (Select one)

Either answer
is correct

- (a) An infrastructure defect
 - (b) The use of social engineering
 - (c) A type of malware
 - (d) The use of a software defect
 - (e) Making transitive trust
 - (f) A magic attack
- For malicious purposes

Question 4: Which one in the following statements is not a vulnerability? (select one)

- (a) Using virus detection software
- (b) Having untrained employees in security
- (c) Having incorrect or incomplete security procedures
- (d) Using untested software
- (e) Using malicious code



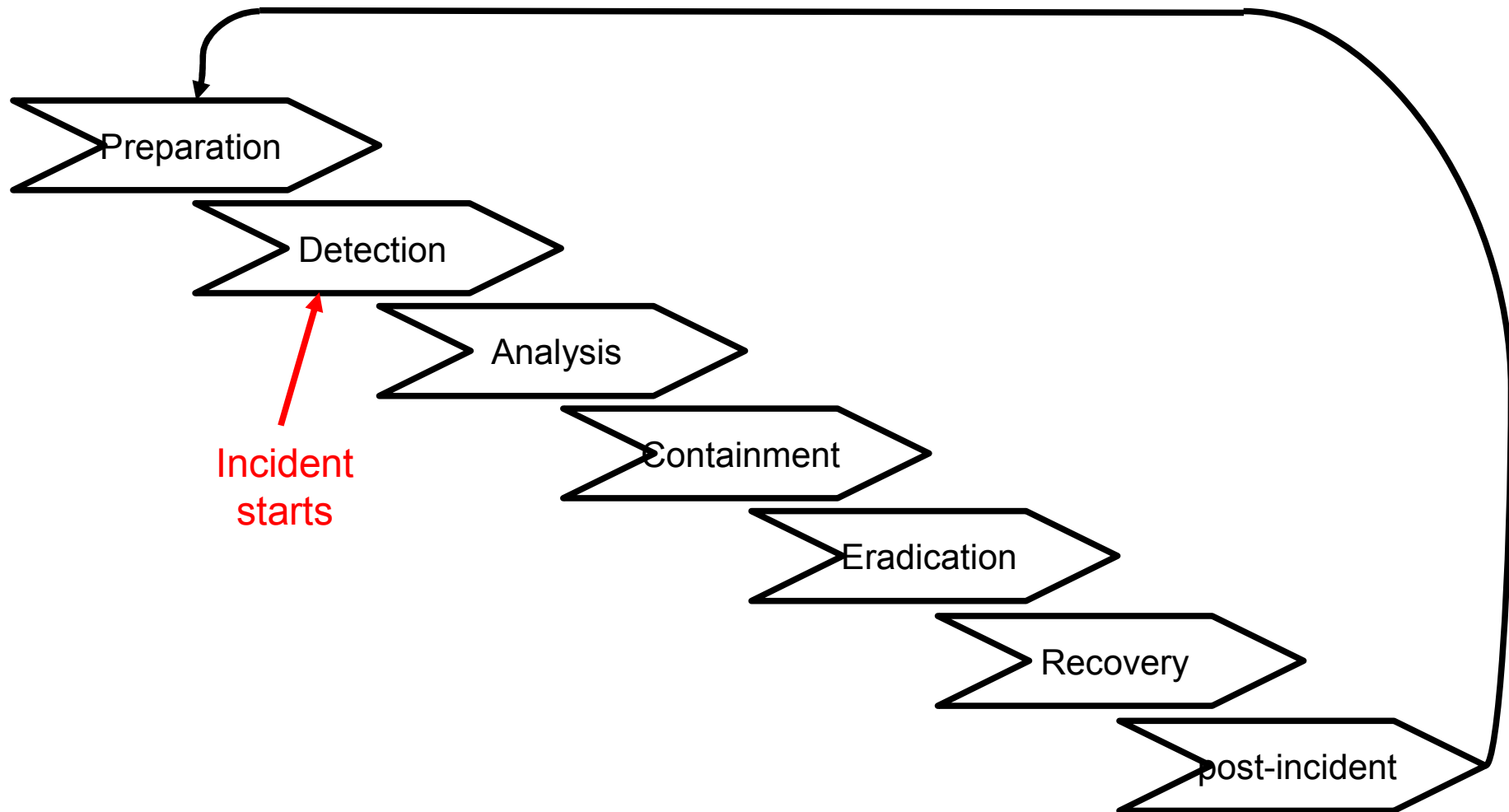
Lesson 14 Review



Security incident

- A violation or imminent threat of violation of security policies, acceptable use policies, or standard security practice
- Examples
 - Denial of Service
 - Malicious code
 - Unauthorized access
 - Inappropriate usage

Incident investigation lifecycle



- Based on NIST SP800-61rev1
- (<http://csrc.nist.gov/publications/PubsSPs.html>)

Second half of the semester 2/2

- Week 14 (4/23)
 - Quiz and Incident Investigation.
 - Project discussions
- Week 15 (4/30)
 - Regulations, Standards, Legal, Ethical, & Professional Issues
- Week 16 (5/07)
 - Project presentations
 - Course review
- Week 17 (5/14)
 - Final Examination




Regulations, Standards, Legal, Ethical, & Professional Issues

Some material from:

Prof. Harry Porter (Portland State University)

Prof. Wu-chang Feng (Portland State University)

Prof. Mike Burmester (Florida State University)



Regulatory acts

- Two major categories of US laws regulating an organization and its IT operation
 - The first group covers core business security regulations, such as:
 - Basel II, Solvency II, IAS/IFRS, and HIPAA.
 - The second group includes the regulation of specific business processes related to IT security, such as:
 - FISMA, CobIT, British Standard 7799 (ISO 17799), Sarbanes-Oxley Act (US), and Homeland Security Act.
- They apply to all companies acting in the U.S. or being registered at stock exchanges.

Common Criteria

- The Common Criteria enables corporate technologists a means of standardizing a common set of requirements for the security functions of IT products.
- Using Common Criteria we can evaluate between different application and appliances judging how best they address an organization's security requirements.
- In 1999, six countries (Canada, France, Germany, Netherlands, United Kingdom, United States) became signatory to Common Criteria 2.0 making it an international standard.
- See the Web site at: <http://www.commoncriteriaportal.org>

Social Legal and Ethical issues

- The impact of computers and computer systems
- The ATM example
 - Unemployment
 - Alienation and customer service
 - Crime
 - Loss of privacy

Social Legal and Ethical issues

Main issues

1. Privacy & personal information
2. Freedom of speech
3. Can we trust computers
4. Intellectual property
5. Computer Crime
6. General social issues
7. Ethics

1. Privacy & personal information

- Freedom from intrusion
- Control information about oneself
- Freedom from surveillance

- Is Big brother watching you?

The fourth Amendment, US Constitution

- The right of the people to be secure in their persons, houses, paper and effects against unreasonable searches and seizures shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Privacy & personal information

- Satellite surveillance and thermal imaging
- Automated toll collection and itemized purchase records
- Search and surveillance tools
- Fighting terrorism

Privacy & personal information

- Protecting Privacy: law & regulation
 - Is there a right to privacy?
 - The free market view vs the consumer protection view
 - Contract and regulations
 - Conflicts with freedom of speech

Free Information and Stuff

- Free Search Engines: Google, Yahoo
- Free Encyclopedia: Wikipedia
- Free Classified Ad: Craigslist
- Free News and Other Articles
- Free Games: chess, bridge, Lego
- Free Phone service: Skype

Free Stuff Problems

- *Hidden Agenda:*
 - Search engine's ranking algorithm
 - Tracking consumer behavior
 - Infomercial vs. hard news
 - Biased or incorrect articles in Wikipedia
- *Harmful Information:*
 - Instructions for bomb making
 - Political attacks

2. Freedom of speech

- Wiretapping
 - Telephone
 - New technologies
- USA Patriot Act 2001:
 - Lets the government collect info from financial institutions on any transactions that differs from a customer's usual pattern, and allows access to the government to many other kinds of personal information without a court order.

Carnivore

- FBI's system for intercepting email
- FBI must first get a court order to intercept someone's email
- The Carnivore system is used at the Suspects Internet Service provider and filters all e-mails from that ISP, examining headers to find suspect email.

NSA's Echelon

- Echelon is similar to Carnivor, but on an international scale.
- Involves a partnership with intelligence agencies of Canada, Britain, Australia and New Zealand, and operates a huge system of listening stations to intercept satellite communication.
 - Targets terrorist and military activities

Should the Internet be filtered/censored?

- Access tightly controlled in
 - **North Korea, Cuba, Myanmar**
- Content tightly controlled in
 - **Saudi Arabia**
 - Centralized control center blocks pornography, gambling, and sites offensive to Islam and the government
 - **China's Great Firewall**
- Special interesting cases
 - Germany banning neo-Nazi web sites
 - US controls pornography
 - Children's Internet Protection Act

Should we have an alternative to Internet?

- Rutgers team has proposed an Internet alternative
 - MondoNet (www.mondonet.org)
 - Decentralized
 - Universally Accessible
 - Censor-Proof
 - Surveillance-Proof
 - Secure
 - Scalable
 - Permanent (Redundancy)
 - Fast (Enough)
 - Independent
 - Evolvable
- There are other alternatives and proposals

3. Can we trust computers ?

- What can go wrong!
 - Billing errors
 - database accuracy
 - failures...
- Increasing Reliability and Safety
 - Overconfidence
 - Redundancy
 - Good design

4- Intellectual Property -- Digital Rights Management

- Problems with new technologies
- Copyright Law
- The fair use doctrine
- Copying Music, Movies, Software Books
 - From floppies to the web
 - The Napster case
 - Beyond Napster
- Software Piracy

Ethical issues

- Fuzziness about the ethics
- Arguments used include:
 - I cant afford to buy
 - The company is a wealthy corporation
 - Too expensive anyway
 - Making a copy from a friend is an act of generosity

5. Computer Crime

- The Law
 - Catching hackers
 - Penalties appropriate to the crime
 - Discouraging and punishing “amateur” hackers
- Design secure “hack-free” systems
- Online scams
 - Chain letters, sale of counterfeit goods, phony investments
 - Collecting credit card numbers, ID and password details
- Fraud, embezzlement, Sabotage
- Identity theft

6. General Social Issues

- Impact on our society
- Information Have's and Have-Nots
 - The digital divide
 - Trends in computer access
 - Abdicating responsibility
- Does the Technology create the need for itself?
 - “... The Web is alive and filled with life, nearly as complex and natural as the primordial swamp...”
- Who benefits most
- Prohibiting bad technologies

Artificial Intelligence (AI)

- “Intelligent” computers / robots / other machines
 - Not today, but perhaps in 20-30 years.
 - Will they have “free will”?
 - Will they become “conscious”?
 - Will they have rights?
- *“They may be very different from humans.”*
 - (This argument has been used to deny rights before!)

Video Surveillance

- Tampa, FL police scanned the faces of all 100,000 attendants of the 2001 Super Bowl.
 - A computer system searched files of criminals for matches, and returned results in seconds (none was found)
 - People were not told that their faces were being scanned
- The UK has one surveillance camera for every dozen citizen. In London, an average person is photographed hundreds of times a day by surveillance cameras.

7- What is ethics?

- A branch of philosophy that studies principles of “right” and “wrong”
- Tries to address questions such as
 - *What does ‘do the right thing’ mean?*
 - *How should people act?*
 - *What rules or laws should we have?*
 - *Should the government spy on citizens?*

Codes of ethical conduct

- Association of Computing Machinery (ACM)
 - One of the two most important professional associations for computer scientists / IT professionals
 - <http://www.acm.org/about/code-of-ethics>
- IEEE Computer Society & ACM:
 - Software Engineering Code of Ethics and Professional Practice
 - <http://www.acm.org/about/se-code/>
- Many others

ACM Code Highlights

- Contribute to society and human well-being
- Avoid harm to others
- Be honest and trustworthy
- Be fair and take action not to discriminate
- Honor property rights including copyrights and patent
- Give proper credit for intellectual property
- Respect the privacy of others
- Honor confidentiality

Discussion questions

- Your company has 25 licenses for a computer program, but you discover that it has been copied onto 80 computers. You informed your supervisor, but he/she is not willing to take any action.
- What would you do next?
 - Give up; you did your best to correct the problem
 - Call the software vendor and report the offense
 - Quit your job
- Are “whistleblowers” heroes or traitors?

The End