CSE 565 Computer Security
Spring 2019

Lecture 21: Security Management

Department of Computer Science and Engineering
University at Buffalo
Lecture Overview

- Physical security
- Risk assessment
- Legal issues
- Privacy
Physical and Infrastructure Security

- Physical threats to computer systems
  - natural disasters
    - tornado, hurricane, earthquake, ice storm, flood, etc.
  - environmental threats
    - inappropriate temperature; fire and smoke
    - water damage; inappropriate humidity
    - infestation, dust, etc.
  - technical threats
    - power problems, electromagnetic interference
  - human-caused physical threats
    - unauthorized physical access, theft, vandalism, misuse
Physical Security

- Threat assessment and planning
  - gather historical information from government agencies, vendors, suppliers, neighboring businesses, etc.
  - identify possible threats
  - for each threat:
    - determine its likelihood
    - approximate direct and indirect costs
    - compute risk factor as: likelihood × total cost (direct plus indirect)
  - prioritize the threats according to their importance
  - develop a plan and implement it
• What measures can be implemented to minimize risks?
  – proper climate control
  – fire detectors and other sensors (water, hazardous materials)
  – positioning of equipment
  – automatic and hand-operated fire extinguishers
  – proper positioning of water supply
  – power-off switch
  – uninterruptible power supplies (UPS), power generators
  – well-known emergency procedures
  – frequently tested emergency equipment
  – anti-theft measures (restricted access, secured facilities)
Overall IT Security Management

- **IT security management** is used to achieve and maintain crucial security goals within an organization
  - confidentiality, integrity, availability, accountability, and reliability

- **Security management functions** include
  - determining security objectives and policies
  - determining security requirements
  - identifying and analyzing threats to assets and risks
  - developing and implementing appropriate security measures
  - monitoring implementation and operation, devising adjustments as necessary
  - detecting incidents and reacting to them
• **IT security management** is a cyclic never ending process
  
  – constantly monitor the system and revise any necessary components
  
  – be aware of new threats and attacks with rapidly changing technology and environment
• Risk assessment
  – to devise proper protection mechanisms, we first need to perform risk analysis
  – as a first step, identify assets and their threats

• Risk is computed as the product of the probability that a threat occurs and the cost to organization
  – often, exact numbers are difficult to identify
  – use approximations instead
  – e.g., likelihoods can be chosen from the set extremely unlikely, unlikely, possible, likely, almost certain
  – cost or consequences can be chosen from minor, moderate, major, and catastrophic
• The resulting risk level can be determined using a table such as

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Consequences</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Catastrophic</td>
<td>Major</td>
<td>Moderate</td>
<td>Minor</td>
</tr>
<tr>
<td>Almost certain</td>
<td>extreme</td>
<td>extreme</td>
<td>extreme</td>
<td>high</td>
</tr>
<tr>
<td>Likely</td>
<td>extreme</td>
<td>extreme</td>
<td>high</td>
<td>high</td>
</tr>
<tr>
<td>Possible</td>
<td>extreme</td>
<td>extreme</td>
<td>high</td>
<td>medium</td>
</tr>
<tr>
<td>Unlikely</td>
<td>extreme</td>
<td>high</td>
<td>high</td>
<td>low</td>
</tr>
<tr>
<td>Very unlikely</td>
<td>high</td>
<td>high</td>
<td>medium</td>
<td>low</td>
</tr>
</tbody>
</table>

• Treat risks according to their priority
  – several possibilities
    • risk acceptance
    • risk avoidance
    • risk transferal
• Decision whether to accept or avoid a risk depends on the cost of treatment.

- Other risk treatment possibilities
  - reduce consequence
  - reduce likelihood
• Identified measures can be implemented through a variety of mechanisms
  – management controls
  – operational controls
  – technical controls

• Each category may include controls for both prevention of security breaches and their detection

• Incident response must be an integral part of the plan
• Wide computer use influences the law and we must be aware of legal and ethical aspects of computer security

• Examples of computer-related laws
  – digital signatures
  – posted contents
  – gathering and dissemination of user personal information (privacy)
  – intellectual property
  – computer crime
Legal Aspects

- **Computer crime**
  - many types of computer attacks can be considered crimes and carry criminal sanctions
  - the US law and international Convention on Cybercrime categorize computer crime based on the target and actions

- Computers can be used as
  - target of attack
    - illegal access, computer-related forgery or fraud
  - storage device
    - storage of stolen credit cards or other sensitive information
  - communication tool
    - traditional crime committed online (illegal sale of drugs, guns, ...)

CSE 565  
Spring 2019  
Marina Blanton
The nature of computer crime makes investigation very difficult
  - low success rate, achieving a consistent success rate is even harder

Unique challenges include
  - investigators need to have a good understanding of technology
  - some investigations require significant resources (computing power, storage, or communications)
  - cybercrime is global and might require cooperation of other law enforcement agencies
  - no cybercriminal database to look for likely suspects
• Low success rate and concerns about corporate reputation result in low reporting rates by cybercrime victims
  – the situation won’t improve without cooperation of organizations
  – law enforcement should be viewed as an additional resource in investigation
  – management needs to understand how the investigation process works and positively contribute to the investigation
• **Intellectual property** (IP) is an asset that consists of knowledge and ideas
  – data, software, music recording, books, technological processes

• Relevant **types of intellectual property**
  – software (copyrighted or patented)
  – algorithms
  – digital contents (music, video, multimedia, web site contents, etc.)
  – databases

• **Enforcement of IP** includes technical measures and legal sanctions
  – access to raw data can be controlled by appropriate interface
  – if user possesses the object, technical security measures are limited
• **Digital Millennium Copyright Act (DMCA)** was signed into law to protect copyrighted material specifically in digital format
  
  – it encourages protection of copyrighted works with technological measures
  
  – it prohibits attempts to bypass such measures
  
  – this includes unauthorized decryption of contents and release of tools that bypass encryption or other protection mechanisms

• **Why does it matter from a security point of view?**
  
  – copyrighted products might have security vulnerabilities
  
  – how can we ensure that their use won’t compromise security of our system?
• The following actions are exempted from DMCA and other laws
  – fair use is allowed for the purposes of review, comment, and discussion
  – reverse engineering of software is allowed if user is authorized to use
    and wants to achieve interoperability (rather than duplication)
  – security testing is allowed for the purpose of correcting security
    flaw/vulnerability with permission of the owner
  – good faith encryption research is allowed
  – technological measures can be bypassed if this is the only reasonable
    way to protect personal privacy

• Despite these exemptions, DMCA is still criticized to hinder legitimate
  security and encryption research
Privacy

• Today **personal information** can be collected in various ways

• Storing it in digital form makes it easy to transfer data to third parties

• **A number of laws exist to protect personal privacy**
  
  – US Privacy Act states rights of individuals when their personal information is collected and used by federal agencies
  
  – personal banking and financial information is protected in certain ways under a number of laws
  
  – medical and health insurance records are protected under the Health Insurance Portability and Accountability Act (HIPAA)
  
  – Children’s Online Privacy Protection Act restricts collection of data from children under 13
• Organizations handling data protected under these laws need to deploy management and technical controls to comply with the law

• Does it mean our privacy is well protected?
  – companies often have vague or ambiguous privacy policies
  – explanation of privacy policies is not easy to get
  – usage of personal information is decided without user consent
    • can always choose not to use the service
    • often can opt out from at least some dissemination of your personal information
  – the government can buy information compiled by non-government companies
• The introduction of new European Union privacy law had a significant impact on companies worldwide

  – EU **General Data Protection Regulation (GDPR)** was signed into the law in 2016 and took effect in May 2018

  – it places users in charge of their data (the right to know how their personal data is used, the right to data erasure)

  – privacy policies and personal data use have to be explained in accessible language

• Since its introduction, GDPR had significant impact worldwide

  – violations of that law are common
• Often computer use is allowed to be anonymous

• Services might still be able to gather information about users

• Various anonymity tools exist to respect personal privacy
  – randomized routing in the internet
    • mixes, proxies, onion routing (TOR)
  – location privacy in other applications
  – pseudonyms in computer systems
  – anonymous credentials for service access