Week 13 - Monday

COMP 4290

Last time

- What did we talk about last time?
- Exam 2 post mortem
- Emerging technologies
  - RFIDs
  - Electronic voting
  - VOIP

Questions?

Project 3

Jennifer Perez Presents

Security Planning

Making a security plan

- What if your boss gives the job of coming up with a plan to protect the computer systems of your company or clients?
- This question is a little more IT than CS, but it still might be a problem you have to deal with

Security plan

- A **security plan** is a document that describes how your organization will address its security needs
- It should address:
  1. Policy
  2. Current state
  3. Requirements
  4. Recommended controls
  5. Accountability
  6. Timetable
  7. Continuing attention

Policy

- A policy is a high-level statement about security
- It should state:
  - Who should be allowed access
  - To which resources access should be allowed
  - What types of access each user should be allowed on each resource
- It should also specify:
  - Security goals for the organization
  - Responsibility for maintaining security
  - Commitment to security: who provides the support
- How could you state the Otterbein student computer policy?

Current security status

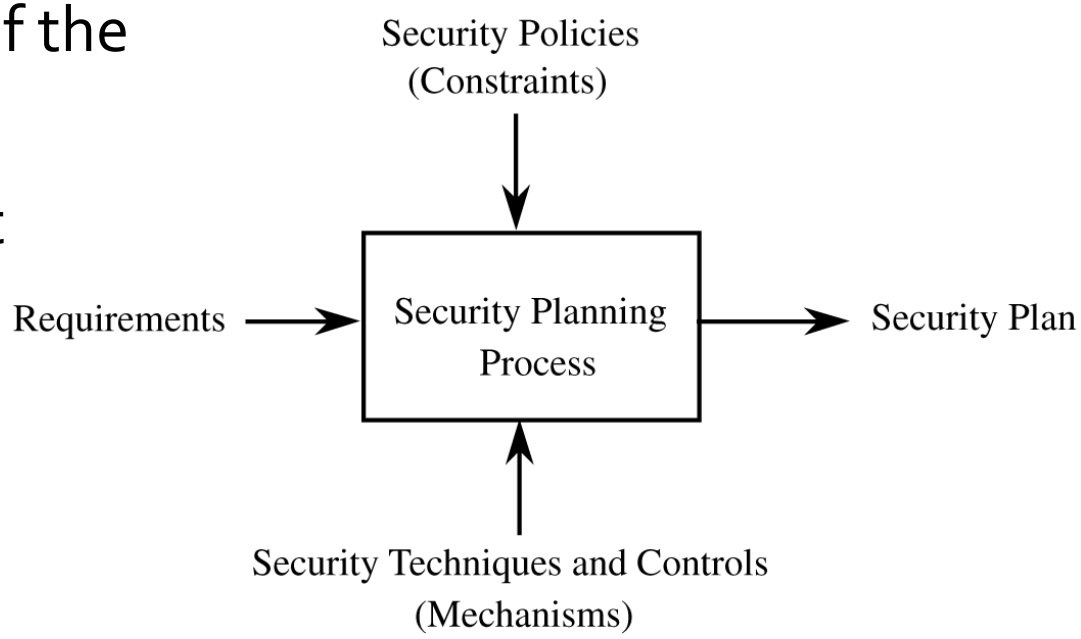
- To plan the security of your company, you need to know how secure it currently is
  - Maybe your company is already pretty secure
- In a few slides, we'll discuss how to do a **risk analysis** to evaluate your company
- Part of examining the current status includes setting limits on what will and won't be covered by your plan

Requirements

- After the preliminaries, **security requirements** are the part of the plan that says what you really have to do
- A requirement is a demand that must be met
  - It doesn't say how that should be done
- Requirements should be:
  - Correct
  - Consistent
  - Complete
  - Realistic
  - Necessary
  - Verifiable
  - Traceable

Recommended controls and responsibility for implementation

- **Controls** are the actual features that we've been discussing all along that are used to meet the requirements according to the **constraints** of the policy
- Controls are not always technical
- They can be implemented by many different employees:
  - Regular users
  - Project leaders
  - Managers
  - DBAs
  - Information officers
- It should always be clear who has what responsibility



Timetable and continuing attention

- Security is complex and cannot be fixed instantly
- The timetable should be realistic
- Part of the plan should call for periodic reevaluation
  - 35 years ago there was no public Internet
  - Technology changes very fast
- Groups that are affected by the plan should be treated with sensitivity and have their role explained

What if something bad happens?

- We have been discussing a security plan for prevention of problems
- A **business continuity plan** covers what will happen if a computer security problem actually happens
- These plans cover big problems
  - Catastrophic situations where large portions of the computer systems don't work
  - They must stop working for a long duration
- Fire, flood, zombie uprising!
  - Except a zombie uprising usually doesn't impact computer security much

Parts of a business continuity plan

- Assess business impact
  - What is absolutely necessary for business to go on?
  - What could disrupt them?
- Develop strategy to control impact
  - There will be tradeoffs
  - What is the most important features to get back up and running?
- Develop and implement a plan
  - Who is in charge
  - What should be done
  - Who does it

Incident security plans

- An **incident security plan** covers the non-business parts of any security breaches
  - There should be incident security plans even for incidents that are too small to fall under a business continuity plan
- Such a plan covers:
  - The definition of an incident
  - Who is responsible for taking charge
  - What the plan of action is
- Such a plan must consider:
  - Legal issues
  - How to preserve evidence
  - How to record the progress in executing the plan
  - How to handle public relations

Risk Analysis

Risk terminology

- **Risk** is the potential for a problem
- Risk is characterized by three factors
  1. Loss associated with the event
     - **Risk impact**
  2. Likelihood that the event will occur
     - A likelihood of 1 means there is a problem
  3. The degree to which we can change the outcome
     - **Risk control** is reducing the risk
- **Risk exposure** = risk impact × risk probability
- We can **avoid**, **transfer**, or **assume** the risk, depending on the tradeoffs

Risk analysis

- **Risk analysis** is examining a system to find vulnerabilities and the harm they could cause
- **Risk leverage** =

$$\frac{(\text{risk exposure before reduction}) - (\text{risk exposure after reduction})}{(\text{cost of risk reduction})}$$

- Steps of a risk analysis:
  1. Identify assets
  2. Determine vulnerabilities
  3. Estimate likelihood of exploitation
  4. Compute expected annual loss
  5. Survey applicable controls and their costs
  6. Project annual savings of control

Step 1: Identify assets

- What is the stuff you want to protect?
- The assets could fall into the categories of:
  - Hardware
  - Software
  - Data
  - People
  - Documentation
  - Supplies
- Other categorizations might include the building or utilities

Step 2: Determine vulnerabilities

- Make a matrix for recording the vulnerabilities for each asset in the areas of confidentiality, integrity, and availability
- For each entry, consider the effects of:
  - Unintentional errors
  - Malicious insiders
  - Outsiders
  - Natural and physical disasters

Asset	Confidentiality	Integrity	Availability
Hardware		Overloaded Destroyed Tampered with	Failed Stolen Destroyed Unavailable
Software	Stolen Copied Pirated	Trojan horse Modified Tampered with	Deleted Misplaced Usage expired
Data	Disclosed Read by outsider Inferred	Damage • Software error • Hardware error • User error	Deleted Misplaced Destroyed
People			Quit Retired Terminated On vacation
Documentation			Lost Stolen Destroyed
Supplies			Lost Stolen Damaged

Step 3: Estimate likelihood of exploitation

- We wish we could use mathematical probability but real security incidents are usually too complex to behave like a pair of dice
- Frequency probability means observing the number of times something happens and using that as a basis
  - We can use previous problems as a guide to future ones
  - Perhaps we can look at similar attacks at similar companies
  - Unfortunately, technology and attacks change quickly
- The **Delphi approach** provides the data to a panel of experts who try to reach consensus about the probabilities

Step 4: Compute expected loss

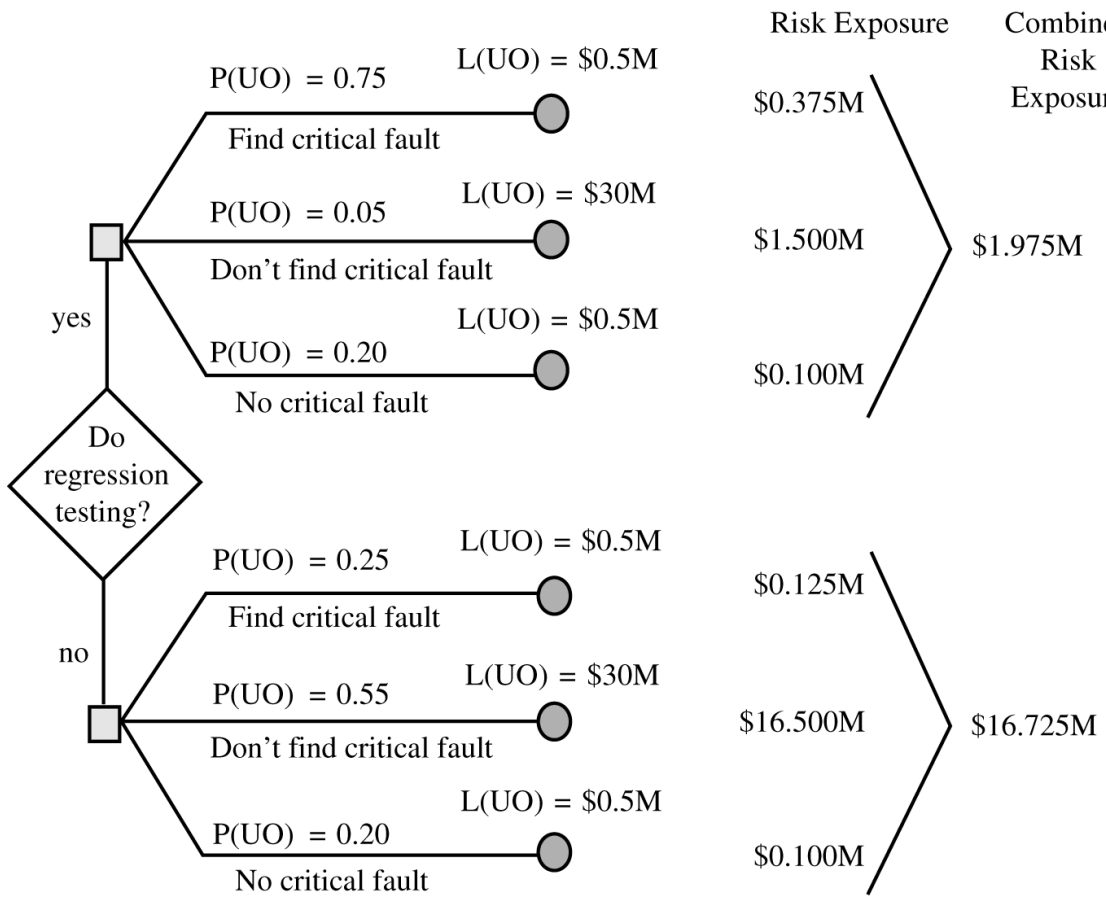
- Cost is not always money, but we can usually convert it to money
- Consider:
  - Legal obligations
  - Business requirements and agreements
  - Harm to a person or organization through a breach of confidentiality
  - Loss of future business opportunities
  - Psychological impact
  - Value of access to computing systems for your company
  - Value of access to your computing systems to outsiders
  - Replacement or reconstruction costs
- What was the job of the guy from *Fight Club*?

Step 5: Survey and select new controls

- Take your existing matrix and then add another dimension for a list of controls under consideration
- Record the effectiveness of each control
- The VAM approach suggests:
  - 2 for a control that significantly mitigates the vulnerability
  - 1 for a control that somewhat mitigates the vulnerability
  - 0 for a control that may have some beneficial side effects
  - -1 for a control that somewhat worsens a vulnerability or creates new ones
  - -2 for a control that significantly worsens a vulnerability or creates new ones
- For tie-breaking, you can consider each control in terms of how it affects the users, implementers, or policy-makers for your systems

Step 6: Project savings

- Businesses are businesses
  - They care about making money
- Security controls usually incur additional cost
- Thorough risk analysis should determine whether adding controls will save money in the long run
- These risks are always statistical
  - You want to look at the average cost based on the probability of the risk being exposed and how that probability is changed by the control



Risk analysis pros and cons

Pros	Cons
Improve awareness	False sense of confidence
Relate security mission to management objectives	Hard to perform
Identify assets, vulnerabilities, and controls	Done once and then forgotten
Improve basis for decisions	Lack of accuracy
Justify expenditures for security	

Organizational Security Policies

Security policies

- A **security policy** is a high level document informing users of the security goals of the system
- Possible purposes:
  - Recognizing sensitive information assets
  - Clarifying security responsibilities
  - Promoting awareness
  - Guiding new users

Focus of a security policy

- Audience
  - Users
  - Owners
  - Beneficiaries
  - The needs of all parties should be balanced
- Purpose
  - Promote efficient business operation
  - Facilitate information sharing in the organization
  - Safeguard information
  - Ensure accurate information is available
  - Ensure a safe workplace
  - Comply with laws and regulations
- The policy should say what is protected and how

Policy Examples

Data Sensitivity Policy

- An (anonymous) company decided to classify all of its data into four levels based on sensitivity
- They instituted separate policies for each level

Classification	Description	Examples
Sensitive	Could damage competitive advantage	• Business strategy • Profit plan
Personal or Protected	Could reveal personal, private, or protected information	• Personal data: salaries, performance reviews • Private data: employee lists • Protected data: data from non-disclosure agreements
Company Confidential	Could damage company's public image	• Audit reports • Operating plans
Open	No harm	• Press releases • Marketing materials

Government Agency IT Security

- I dislike the book's example of the US Department of Energy's security policy
- It is very broad, covering every kind of harm from every source and every kind of control, but in a very general way
- The document goes on to specify what each user, security officer, and manager should do

Internet Security Policy

- The Internet Society made a policy for all users of the Internet:
  - Users are responsible for abiding by the policies for their systems
  - Users are responsible for employing available security mechanisms
  - Service providers are responsible for keeping their systems secure and notifying users of changes
  - Developers are responsible for providing systems with adequate security controls
  - Everyone is responsible for cooperating
  - Researchers should try to improve the security of Internet protocols

Upcoming

Next time…

- Physical security
- Lockpicking
- Legal issues
- Hussein Al-Ani presents

Reminders

- Work on Project 3
  - **Phase 1 due Friday!**
- Read Chapter 11