# Last time

- Data Mining
  - Integrity and Availability
  - Privacy and Data Mining
  - Privacy-Preserving Data Mining

# This time

- Administering Security
  - Security planning
  - Risk Analysis

# Administering security

- So far in this course, we've talked about a lot of things you can do technically to protect your programs, operating systems, networks, databases, and Internet applications
- But there's more to security and privacy than just these technical solutions
- Next, we will look at four non-technical aspects of administering security:
  - Security planning
  - Risk Analysis
  - Security policies
  - Physical security

# Security planning

- It used to be that employees understood that when you went home for the day, you locked up all your files in your filing cabinet
  - What do they do today, now that the files are all electronic?
- Many users do not appreciate the security and privacy risks in using computers
- A security plan is a document put together by an organization that explains what the security goals are, how they are to be met, and how they'll stay met
  - Employees can use this document to inform their actions

# Contents of a security plan

- A security plan is both a description of the current state of the security of an organization, as well as a plan for improvement
- It has seven parts, which we will look at in turn:
  - Policy
  - Current state
  - Requirements
  - Recommended controls
  - Accountability
  - Timetable
  - Continuing attention

# Policy

- A high-level statement of purpose and intent
- The policy statement should specify:
  - Goals
    - Relative importance of confidentiality, integrity, availability
    - Which has higher priority: securing data or serving customers?
  - Responsibility
    - Whose job is getting security right? Every employee's? A security manager? A security group in IT?
  - Commitment
    - Institutionally, who provides security support for staff? Where does security fit into the org chart?

# Current state

- The security plan should contain a risk analysis (see later) describing the current status of the system
  - What assets are there? What might go wrong? What vulnerabilities are currently exposed?
- What should you do if new assets are added?
- List the limits of security responsibility
  - Who is responsible for the security of the Internet uplink router to the company's ISP?

# Requirements

- What needs does the organization have?
  - Who is allowed/not allowed to do what?
  - What audit logs should be kept?
  - Do you need to be able to measure the ongoing effectiveness of the security controls?
- Not anything to do with mechanism
  - The policy statement doesn't say anything about how to accomplish the listed goals
  - It should be technology-neutral
  - For example, it might say that employees should be allowed to access their email while travelling; it should not say any of the words VPN, ssh, TLS, IPSec, etc.

# Recommended controls

- Here's where you list mechanisms to control vulnerabilities identified in the “Current state” section, to satisfy the needs in the “Requirements” section, taking into account the priorities in the “Policy” section.

- They may be any of the security controls we've talked about in this course, or other similar ones
  - Program, OS, Network, Internet application, Database, etc.

# Accountability

- Who is accountable if the security controls aren't implemented, aren't implemented properly, or fail?
  - Desktop users?
  - Project leaders?
  - Managers?
  - Database admins?
  - Information officers?
  - Human resources?
- Probably different people will be accountable for different pieces of the plan

# Timetable

- Any reasonably sized security plan will be too big to implement all at once
  - Obtaining new hardware / software
  - Configuring / installing it
  - Training users
- The timetable section of a security plan lists how and when the elements of the plan will be performed
  - What order, noting dependencies
- Include milestones to track progress along the way

# Continuing attention

- The state of the organization isn't static
- The state of the world isn't static
- There will be new vulnerabilities
- Existing controls will become ineffectual
- The security plan should list a process for periodic review and updating of the plan itself

# Who writes the security plan?

- Who performs the security analysis, makes recommendations, and writes the security plan?
- The security planning team should have representation from a number of different constituencies:
  - Upper management / CTO / CIO (setting policy)
  - IT (hardware group, sysadmins)
  - Systems and application programmers, DB admins
  - Data entry personnel
  - Physical security personnel
  - Representative users

# Business continuity plans

- The Business Continuity Plan (BCP) is another kind of security plan
  - Focus is on Availability
- What will your organization do if it encounters a situation that is:
  - Catastrophic: a large part (or all) of a computing capability is suddenly unavailable
  - Long duration: the outage is expected to last for so long that business would suffer if left unattended

# Catastrophic failures

- Some examples of such failures:
  - Fire / earthquake destroys your data centre
  - A utility (phone, network, electricity, etc.) fails or goes out of business
  - Flood prevents operations staff from being able to reach your offices
  - Pandemic outbreak of avian flu keeps 1/3 of your staff home sick
    - See UW's pandemic plan (listed as a reading)
- What do you do?
  - Consult your business continuity plan

# Don't blame “the computer”

- If your business can't go on because some computer isn't working right, that's not the computer's fault; it's yours, for not having a backup contingency
  - Some (physical) stores can't sell you goods if their computers are down
  - Better stores have a fallback procedure where they keep track of sales on paper until the computer comes back up and the accounts can be reconciled

# Advance planning

- You need to write an actual plan, which should include things like:
  - Who is in charge when a catastrophe occurs
    - This person will also be the one to declare when the emergency is over and things can get back to normal
  - What needs to be done
    - To deal with *keeping the business going*, not with *dealing with the emergency itself*; someone else will do things like call the fire department
  - Who will do it

# Advance planning

- But writing the plan isn't enough! Before something occurs, you need to:
  - Acquire redundant equipment
  - Arrange for regular data backups
  - Stockpile supplies
  - Train employees so that they know how to react
    - This may also involve live testing of the BCP

# Incident response plans

- You notice that your company's home page has been defaced
- What do you do?
- Follow your company's incident response plan
  - “Incident” in this case refers to a security breach

# Incident response plans

- The incident response plan needs to consider a number of things
  - Legal issues
    - The incident has legal ramifications. Under what circumstances should law enforcement get involved?
  - Preserving evidence
    - How can you quickly recover from the incident while maintaining as much forensic evidence as possible?
  - Records
    - Keep careful track of everything you do once you notice the breach
  - Public Relations
    - Speak with one voice

# After the incident

- Once you have recovered from the incident, hold a review to ask:
- Is any security control action to be taken?
  - How did the breach occur? Have you patched that particular hole? Have you established procedures so that other similar problems are less likely to happen in the future? Was lack of user training an issue?
- Did the incident response plan work?
  - Did everyone know whom to notify? Did the response team have the needed resources? Was the response fast enough? What should be done differently next time?

# Risk

- A risk is a potential problem that a system or its users may experience
- Risks have two important characteristics:
  - Probability: what is the probability (between 0 and 1) that the risk will occur? (That is, the risk will turn into a problem)
  - Impact: if the risk occurs, what harm will happen? This is usually measured in terms of money (cost to clean up, direct losses, PR damage to the company, etc.)
- The risk exposure = probability x impact
- Note that both probability and impact of a given risk will change over time, so continual review is needed

# Risk analysis

- It is impossible to completely eliminate risk
  - No system is absolutely secure
  - Even in your daily life, there are risks all around you
    - Crossing the street?
  - We perform risk analysis to determine if the benefits of some action outweigh the risks
    - If not, is there anything we can do to reduce the risk exposure, either by controlling the probability or reducing the impact?
- As you can see, risk analysis is not specific to security and privacy issues
  - But bringing risk analysis to those issues is a relatively new, and extremely useful, phenomenon

# Risk analysis

- In our setting, a risk analysis usually comprises the following steps:
  - Identify assets
  - Determine vulnerabilities
  - Estimate likelihood of exploitation
  - Compute expected loss
  - Survey applicable controls
  - Project savings due to control

# Identify assets

- Way back in lecture 1, we identified three main assets we would want to protect:
  - Hardware, software, data
- Here, we add three more
  - People
    - Skills to run the system, network, or specific programs
  - Documentation
    - On hardware and software, but also the security plan, business continuity plan, and incident response plan
  - Supplies
    - Paper, forms, printer toner, etc. that play a supporting role

# Determine vulnerabilities

- This step is where you best apply the knowledge obtained in this course
- “Think like an attacker” and be very creative
  - Even outlandish; this part can be fun!
- Come up with as many attacks on your own systems as you can, both technical and non-technical, against assets in each of the six categories
  - Confidentiality, integrity, availability
  - Don't forget privacy issues as well

# Estimate likelihood of exploitation

- This is the hardest step, and there are experts trained in doing it
- It's difficult to estimate the probability of each risk
  - Especially if it's so unlikely that it's never happened before
  - Otherwise, frequency analysis can be useful
    - How often has this risk been a problem in the past?
  - Distinguish something that might happen once a year from something that might happen once a month
- Take into account existing controls and their own probabilities of failure

# Compute expected loss

- Identify the impact of the risk
- Also a tricky step (even though estimates are usually good enough)
- Some examples:
  - Legal obligations to conserve confidentiality or integrity
  - Penalties for failing to provide a service
  - Could release of data cause harm to a person?
  - Value of keeping data out of competitor's hands
    - Different from value of data to competitor
  - Cost of delaying or outsourcing data processing if your systems are unavailable

# Survey applicable controls

- For each risk, think of different ways to control the vulnerability
  - Again, both technical and non-technical means
- Classify each control as to how well it protects against each vulnerability
  - Note that a control that protects against one vulnerability might make another one worse!
  - Also watch out for interactions among different controls

# Project savings due to control

- The expected cost of not controlling the risk is just the risk exposure, as computed earlier
- For each control, the cost of the control is its direct cost (for example, buying the network monitoring equipment, training, etc.), plus the exposure of the controlled risk
  - Most controls aren't perfect: even with the control, there will still be a (smaller, hopefully) probability of a problem
- Savings = Risk exposure – Cost of control
  - Hopefully, this is positive

# Recap

- Administering Security
  - Security planning
  - Risk Analysis

# Next time

- Physical security
- Legal and ethical issues