Risk Management and Incidents

Computer Security
1DV700

Faiz Ul Muram, Ola Flygty
Linnaeus University, Sweden
{faiz.ulmuram, ola.flygty}@lnu.se

Objectives and Contents

- This lecture gives a brief overview of administering security by looking at following areas:
  - Organizational Security Policy
  - Security Planning
  - Business Continuity and Incident Response Planning
  - Risk Analysis
  - Threat Modelling
  - Physical Security

Organizational Security Policy

- Security policy a high-level management document that formally defines security goals, rules, and constraints on using a system
  - What sensitive information assets?
  - What is and isn't allowed? Who should be allowed access?
  - Clarifying security responsibilities
  - Promoting awareness for existing staff and giving guidelines to new employees

- Compliance with laws and regulations
- The organization as a whole primarily focused on maintaining **confidentiality** of data, information **integrity**, certain systems in that organization may rightfully focus on **availability**

Organizational Security Policy: Audience, Contents

A security policy should address the following:

- **Audience**: who can access?
  - Audience can be classified into users, owners, and beneficiaries (e.g., customers, clients)

- **Contents:** which resources?
  - A risk analysis identifies the assets (resources) that are to be protected
    - The assets should be listed in the policy document, e.g., computers, networks, general data
  - The policy should also indicate
    - **who** should have **access** to the protected resources
    - **how** that access will be **ensured** and
    - **how** unauthorized people will be **denied access**

Organizational Security Policy: Characteristics

- **Characteristics** of a good security policy
  - **Coverage**: a security policy must be comprehensive, and general enough to apply to new cases
  - **Durability**: a security policy must grow and adapt well
  - **Realism**: it must be possible to implement the stated security requirements with existing technology
  - **Usefulness**: it must be clear, direct, and understood

Security Planning

- Every organization using computing resources should perform thorough and effective security planning
- A security plan is both an official record of current security practices and a blueprint for orderly change to improve those practices
- To define and implement a security plan three aspects will be considered:
  1. Contents of a security plan
  2. Who are involved in planning
  3. How to guarantee support for a plan

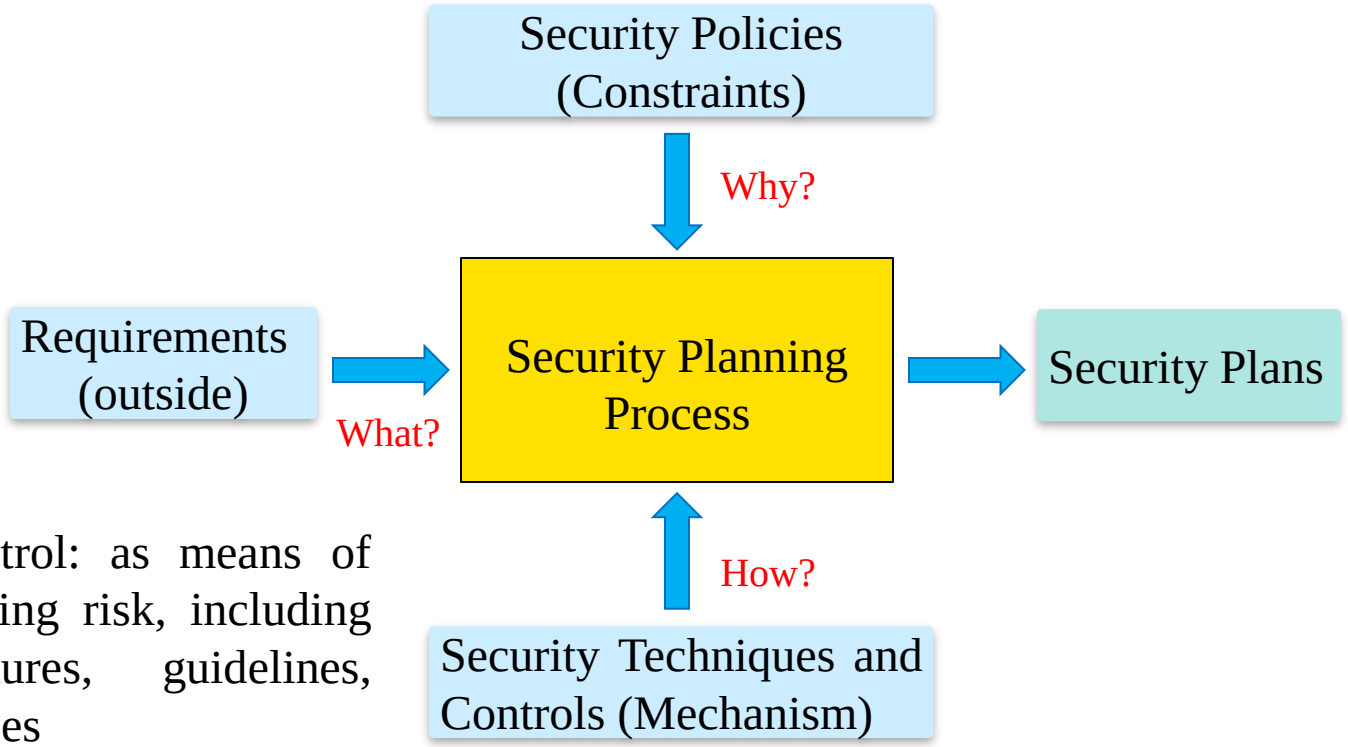
Requirements for Security Planning

- Before we start the work of creating a security plan there should already be some policy documents in place:
  - Business policy/vision
  - Information Security policy
  - IT Security policy
- A security **policy** identifies the rules that will be followed to maintain security in a system
- A security **plan** details how those rules will be implemented
- Characteristics of good security requirements:
  - Correctness, Consistency, Completeness, Realism, Need, Verifiability, Traceability

Contents of a Security Plan

- **Policy** describes the security goals and the willingness of the people involved to work to achieve those goal
- **Current state** representing the status of security at the time of the plan
- **Requirements** recommend the ways to meet the security goals
- **Recommended controls**, mapping controls to the vulnerabilities identified in the policy and requirements
- **Accountability** who is responsible for each security activity in the case of failure, e.g., responsibilities for desktop users, DB admins
- **Timetable** when different security functions are to be done
- **Maintenance** specifying a structure for periodically updating the security plan

Inputs to the Security Plan



A control: as means of managing risk, including procedures, guidelines, practices

Security Planning: Responsibility for Implementation

- The plan should identify who are responsible for implementing the security requirements
- Different stakeholders are responsible for different security roles. For example:
  - **Users**: personal computers responsible for the own machines, laptops
  - **Project leaders**: data and computations
  - **Managers**: seeing that the people they supervise implement security measures
  - **Database administrators**: access to and integrity of data in databases
  - **Information officers**: creation and use of data; retention and proper disposal of data
  - **Personnel staff members:** may be responsible for security involving employees

Security Planning: Team Members

- The planning team should represent each of the following groups depending on the type of organization
- Common security planning representation:
  - Computer hardware group
  - System administrators
  - Systems programmers
  - Applications programmers
  - Data entry personnel
  - Physical security personnel
  - Representative users

Security Planning: Guarantee Support

- Ensuring that security functions will be implemented, and security activities carried out
- Three groups of people must contribute to making the plan a success:
  - The planning team
  - Those affected by the security recommendations
  - Management: using and enforce the security

Business Continuity and Incident Response Planning

Business Continuity Planning

- A business continuity plan documents how a business will continue to function during or after a computer security incident
- Business continuity plan addresses situations having two characteristics:
  - ***Catastrophic situations***, in which all or a major part of a computing capability is suddenly unavailable (e.g., fire, flood,…)
  - ***Long duration***, in which the outage is expected to last for so long that business will suffer

Continuity Planning Activities

- Assess the business impact of a crisis
  - What are the essential assets?
  - What could disrupt use of these assets?

- Develop a strategy to control impact
  - Investigate how the key assets can be safeguarded (e.g., a backup copy of data,…)

- Develop and implement a plan for the strategy
  - Define:
    - Who is in charge when an incident occurs
    - What to do when an incident occurs
    - Who does what tasks when an incident occurs

Incident Response Plan (IRP)

- A security incident response plan tells the staff how to address security incidents
  - monitoring, detecting, analyzing information security events and incidents, discussing observations, and sharing information across the company

- In contrast to a business continuity plan, the goal of incident response is handling the current security incident without direct regard for the business issues
- An incident response plan should
  - Define what constitutes an incident
  - Identify who is responsible for taking charge of the situation
  - Describe the plan of action

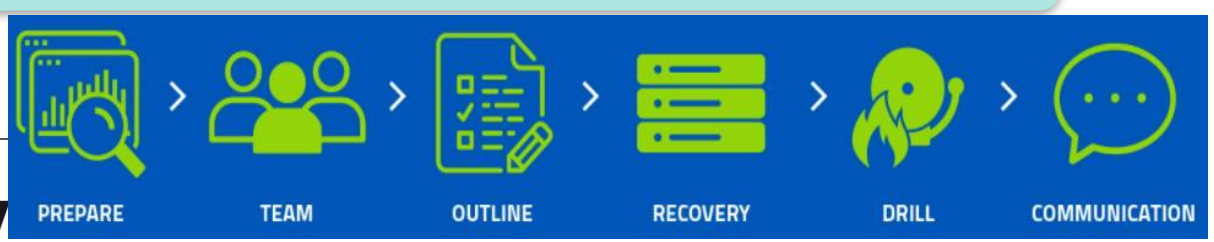


Figure taken from Internet

Computer Security Incident Response Teams (CSIRTs)

- CSIRTs or computer emergency response teams (CERTs) are teams trained and authorized to handle security incidents
- Responsibilities of a CSIRT include
  - **Reporting:** Receiving reports of suspected incidents and reporting as appropriate to senior management
  - **Monitoring and Detecting Incidents**: Investigation to determine if an incident occurred, determine the root cause
  - **Triage (prioritize)**: Immediate action to address urgent needs
  - **Response**: Coordination of effort to address all aspects in a manner appropriate to severity and time demands
  - **Postmortem**: Declaring the incident over and arranging to review the case to improve future response, providing reports to management
  - **Maintaining awareness**: Preventing harm by advising on good security practices and disseminating lessons learned from past incidents



CSIRT Skills

- At different times response teams need a variety of skills, including the ability to
  - Collect, analyze, and preserve digital forensic evidence
  - Analyze data to infer trends
  - Analyze the source, impact, and structure of malicious code
  - Help manage installations and networks by developing defenses such as signatures
  - Perform penetration testing and vulnerability analysis
  - Understand current technologies used in attacks

Risk Analysis

Recall Definitions

- **Asset:** Anything useful or valuable worth protecting
- **Vulnerability:** Weakness or lack of protections
  - Design/implementation flaw – e.g., missing input validation
  - Deployment/configuration issue – e.g., default passwords
  - Feature misuse – HTML in email to disguise a phishing link
- **Threat:** Something that could negatively impact an asset
- **Security Controls**: Protect against threats, reduce vulnerability
  - processes and measures that help enforce the policy; prevent violations, detect violations and limit damage; handle recovery

Risk Analysis

- Identifying the most significant risks in a computing environment, determining the impact of those risks, and weighing the desirability of applying various controls against those risks
  - ***Risk Impact*** associated with an event loss
  - The **probability** (likelihood of occurrence) $\boldsymbol{P_{risk}}$

    0=< $\boldsymbol{P_{risk}}$ <=1 ; When $\boldsymbol{P_{risk}}$ = 1 we say there is a problem
  - ***Risk Control*** involves a set of actions to reduce or eliminate the risk

Strategies for Dealing with Risk

- **Avoid** the risk by changing requirements for security or other system characteristics
- **Transfer**
  - the risk by allocating the risk to other systems, people, organizations, or assets or
  - by buying insurance to cover any financial loss should the risk become a reality
- **Assume** the risk by accepting it, controlling it with available resources, and preparing to deal with the loss if it occurs

Risk Analysis

- The effects of a risk can be quantified by multiplying the risk impact by the risk probability, yielding the risk exposure

$$\textbf{\textit{Risk Exposure}} = \textbf{\textit{Risk Impact}} * \boldsymbol{P_{risk}}$$

- Example if the likelihood of getting infected with malware):

  $\boldsymbol{P_{risk}}$ = 0.40;

  Risk Impact =10,000 Kr (cost of cleaning the affected files)

  Risk Exposure = 0.4 * 10000 = 4000 Kr

So, we could potentially, based on this calculation, decide an antivirus software worth 400 Kr is worth an investment!

Risk Leverage

- In addition to costs of risk's potential impact, the costs are to reduce it
- Risk leverage is the difference in risk exposure divided by the cost of reducing the risk
- If the cost high the leverage will be low

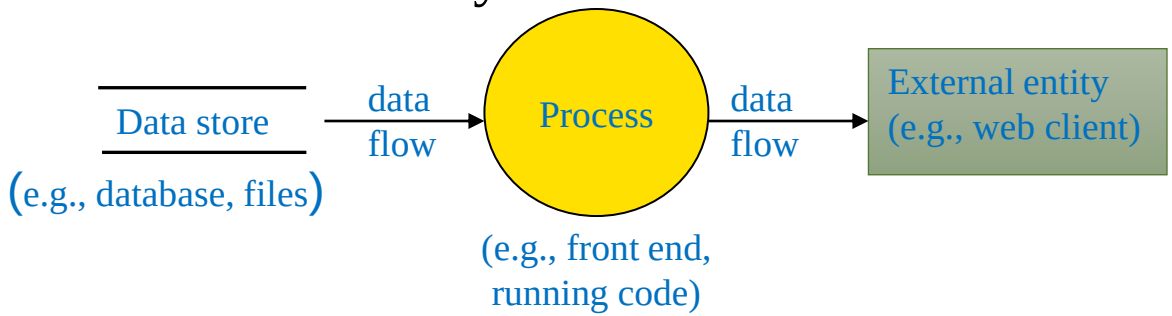
$$\frac{(risk\ expore\ before\ reduction) - (risk\ expore\ asfter\ reduction)}{(cost\ of\ risk\ reduction)}$$

Threat Modelling

- Threat modeling is a process by which potential threats, such as structural vulnerabilities can be identified, enumerated, and prioritized (risk modelling)
- The purpose of threat modeling is to provide defenders with a systematic analysis of the probable attacker's profile, e.g., the assets most desired by an attacker
- Threat modeling methods are used
  - to create an abstraction of the system;
  - profiles of potential attackers, including their goals and methods;
  - catalog(s) of potential threats that may arise

Threat Modelling: Data Flow Diagram

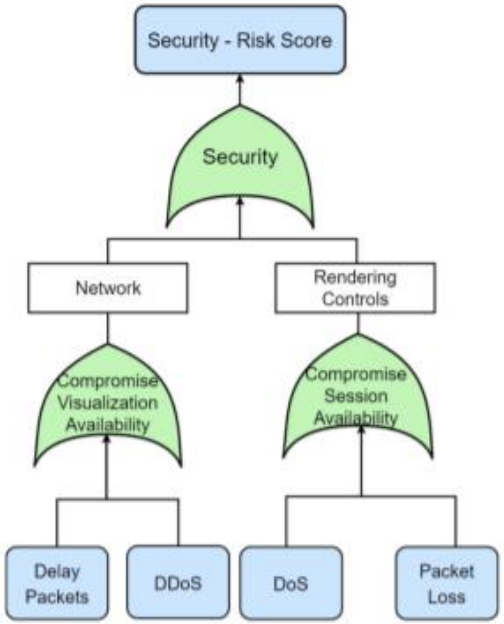
- Analyzing the application/System. What does the system do?
- Data Flow Diagrams (DFDs) to describe how data enters, leaves and traverses the system



- The goal of diagrams is to communicate how the system works, so that everyone involved in threat modeling has the same understanding
- Discover misunderstandings about the security of the system
  - *Where and how can bad things happen? What could go wrong?*
  - *Where is sensitive data stored? Are there non-standard paths?*

Threat modelling: Attack Tree

- Attacks trees were defined by Bruce Schneier to model threats against computer systems
- Hierarchical decomposition of a threat
- In an attack tree model, the topmost (root) node represents an objective or goal
- Sub-nodes – potential means of reaching the goal
  - AND – all of the sub-nodes must be true for the goal to be achieved
  - OR – any one of the sub-nodes must be true for the goal to be achieved
- The atomic nodes are known as leaf nodes and represent the actual actions performed by an attacker



Gulhane et al. 2019. Security, Privacy and Safety Risk Assessment for Virtual Reality Learning Environment Applications

Threat Modelling: STRIDE

- **STRIDE** provides 6 threat categories to support threat identification

1. **Spoofing**
   - Impersonating someone, pretending to be someone else, e.g., faking the sender field of an e-mail; using another person's username and password
   - Violates authentication
2. **Tampering**
   - Modifying data (in storage or in transit), e.g., changing files or DB entries, dropping network packets
   - Violates integrity
3. **Repudiation**
   - Denial of an action, not acknowledging responsibility, e.g., denying approving an expense report
   - Violates auditability, non-repudiation (actions of users cannot be refuted)

Threat Modelling: STRIDE

4. **Information disclosure**
   - Allowing access to data to unauthorized users, e.g., selling company secrets, failing to set up authorization for a database
   - Violates confidentiality
5. **Denial of service (DoS)**
   - Preventing a system from providing a service, e.g., by consuming system resources; a distributed DoS attack uses up all available network connections
   - Violates availability
6. **Elevation of privilege**
   - Doing something not allowed at the current level of authorization, e.g., user code running with admin privileges; accessing the business logic directly instead of through the web interface
   - Violates authorization

Steps for Risk Analysis

Risk analysis usually comprises the following steps:

- **Identify assets:** what we need to protect
- **Determine vulnerabilities:** predict what damage might occur to the assets and from what sources
- **Estimate likelihood of exploitation:** how often each exposure is likely to be exploited
- **Compute expected loss:** determine the likely loss if the exploitation does indeed occur
- **Survey applicable controls:** see which controls address the risks identified in previous steps
- **Project savings due to control:** determine whether the costs outweigh the benefits of preventing or mitigating the risks

Identify Assets

- Asset identification should be performed at a suitable level of detail that provides sufficient information for the risk assessment
- **Hardware:** Processors, monitors, terminals, microcomputers, workstations, tape drives, printers, disks, connections, communications controllers, …
- **Software:** Programs (such as source, purchased, in-house, utility), operating systems, systems programs (such as compilers), and diagnostic programs
- **Data:** Data used during execution, stored data on various media, printed data, archival data, update logs, and audit records
- **People:** Skilled staff needed to run the computing system or specific programs, as well as support personnel such as guards

Identify Assets

- **Documentation:** On programs, hardware, systems,…
- **Supplies:** Form, recordable media, and printer ink, as well as power, heating and cooling, and necessary buildings or shelter
- **Reputation:** Company image
- **Availability:** Ability to do business, ability to resume business rapidly and efficiently after an incident

Determine Vulnerabilities

- Finding weaknesses, we can predict what damage might occur to the assets and from what sources
- A vulnerability is any situation that could cause loss of confidentiality, integrity, and availability

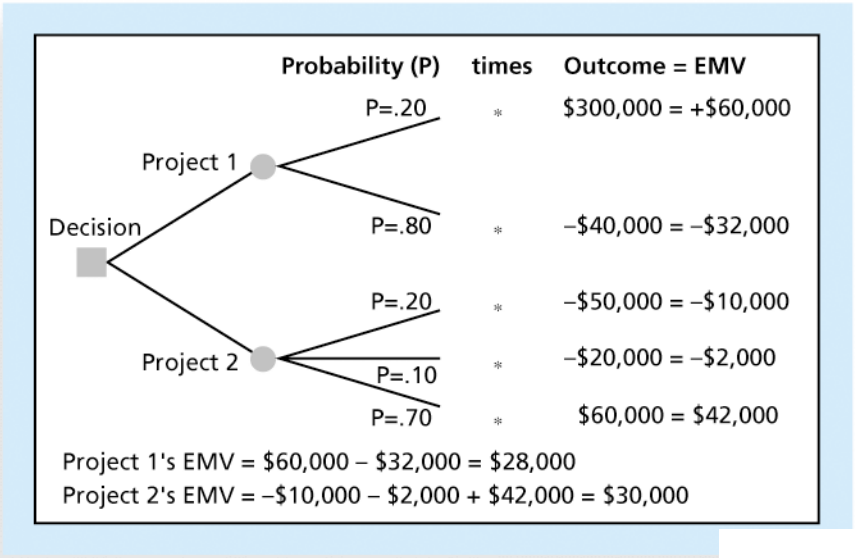
Asset	Secrecy	Integrity	Availability
Hardware		overloaded destroyed tampered with	failed stolen destroyed unavailable
Software	stolen copied pirated	impaired by Trojan horse modified tampered with	deleted misplaced usage expired
Data	disclosed accessed by outsider inferred	damaged - software error - hardware error - user error	deleted misplaced destroyed
People			quit retired terminated on vacation
Documentation			lost stolen destroyed
Supplies			lost stolen damaged

Matrix Mapping CIA to Asset

Estimate Likelihood of Exploitation

- Because it is impossible to know all of a system's vulnerabilities or all the ways those vulnerabilities can be exploited, is also impossible to accurately assess likelihood of exploitation
- Possible approaches to estimation:
  - Look at historical data
  - Use an analyst familiar with such systems to estimate number of occurrences in a given time period
  - Use descriptive adjectives or a simple rating system
  - The Delphi approach (a group of experts come to a consensus about the likelihood of different risks)

Risk Analysis Methodologies



Quantitative risk analysis

- **Quantitative risk analysis**: numbers can be assigned to estimating the expected losses (various risks)
- The total cost of a defense should not exceed the anticipated benefit (i.e., the expected loss)

- **Qualitative risk analysis**: descriptive adjectives are used to rate risks, so one risk might be categorized as certain, likely, possible, unlikely or rare

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Compute Expected Loss

- In addition to the obvious costs, such as the cost to replace a hardware asset, there are hidden costs:
  - Cost of restoring the system to a previous state
  - Cost of downtime
  - Legal fees
  - Loss of reputation and confidence
  - Loss of confidentiality
- Some hidden costs may be impossible to accurately evaluate, but considering them will nonetheless aid in risk management

Survey and Selecting Controls

- Once you understand your assets, vulnerabilities, estimated likelihood of exploitation, and cost of exploitation, you have enough information to select controls
- Controls can be selected from **ISO/IEC 27002** standard or from other control sets, or new controls can be designed
  - For instance, testing of security functionality, test case
  - Rules for the development of software and systems
- Each vulnerability may have one or more controls associated with it, and each control may work for many assets and multiple vulnerabilities

Project Costs and Savings

- This step is meant to determine whether the costs of implementing controls outweigh the expected benefits
- The effective cost of a given control is the actual cost of the control (including purchase price, installation and deployment costs, and training costs) **minus** the expected loss the control is expected to prevent
- The cost may be positive if the product is very expensive or introduces new risks to the system, or it may be negative if the expected reduction in risk is greater than the cost of the control

Note that the reduction of cost from combination of several controls can not simply be added up!

Example: Access Control Software Cost

Item	Amount
Risks: disclosure of company confidential data, computation based on incorrect data	
Cost to reconstruct correct data: $1,000,000 @ 10% likelihood per year	$100,000
Effectiveness of access control software: 60%	– 60,000
Cost of access control software	+25,000
Expected annual costs due to loss and controls (100,000 – 60,000 + 25,000)	$65,000
Savings (100,000 – 65,000)	$35,000

Risk Exposer = Risk impact * P_risk

Impact * P_risk

Impact * Probability after control

Exposure – Exposure after reduction/ cost of control

Risk	Control	Impact	Probability	Exposure	Cost of control	Probability after control	Exposure after reduction	Leverage	Savings
1	I	10000	0.1	1000	100	0.095	950	0.5	-50
	II	10000	0.1	1000	500	0.05	500	1	0
	III	10000	0.1	1000	2000	0.03	300	0.35	-1300
2	III	100000	0.25	25000	10000	0.1	10000	1.5	5000
	IV	100000	0.25	25000	2000	0.2	20000	2.5	3000
3	V	500	0.8	400	100	0.1	50	3.5	250
	VI	500	0.8	400	200	0.2	100	1.5	100

Exposure – Cost of control – Exposure after reduction

Physical Security

- There are many threats outside the computer system security
- Physical security can be in one of these forms:
  - Humans: unauthorized access, stealing and use
  - Natural disasters: fire, flood, earthquake, storms, etc.
  - Power Loss

- Control: Typical physical security controls include alarms, locks, cameras, fences to deter direct attacks
  - Entry or exit controls to ensure that only authorized personnel are allowed access
  - Install suitable intruder detection systems

- Contingency Planning is the key to successful recovery
  - Backup permits recovery from loss or failure of a computing device
    - Offsite backup keeping a backup version separate from the actual system reduces the risk of its loss
    - Cloud backup companies, including Google, and Amazon, effectively augment a user's workstation with a seemingly infinite set of hardware on the Internet

References

- Pfleeger and Pfleeger 2015, *Security in Computing*, 5th ed
- Adam Shostack 2014, *Threat Modelling: Designing for Security*
- Lecture by Jennifer Ferreira, Ian Welch, Harith Al-Sahaf, Victoria University of Wellington
- Lecture by Matus Nemec, Linköping University
- ISO/IEC 27005, Information technology — Security techniques — **Information security risk management**

Lnu.se