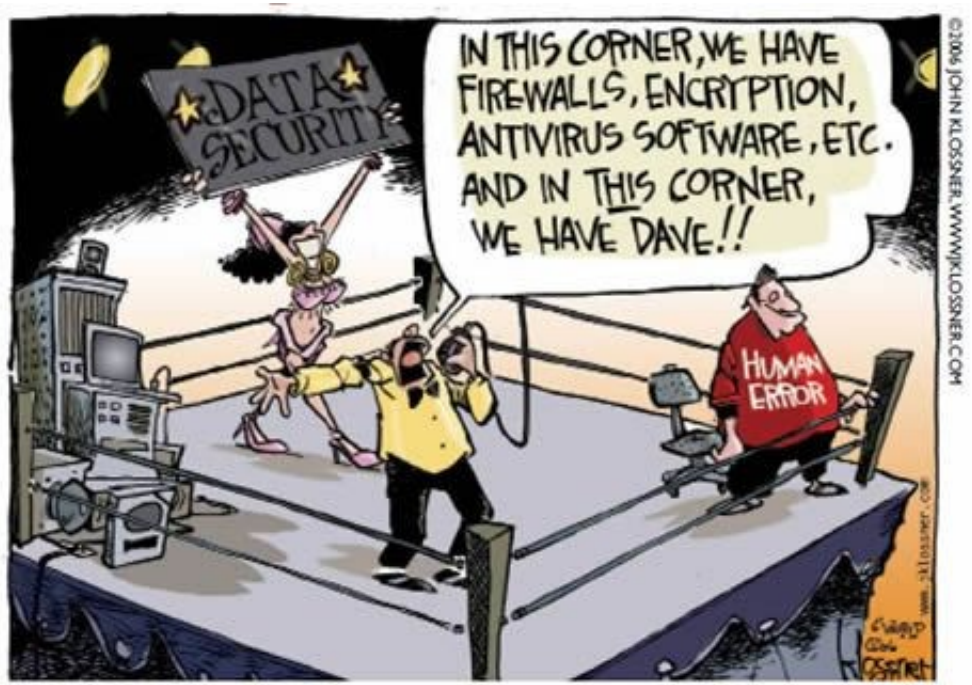
Administering Security

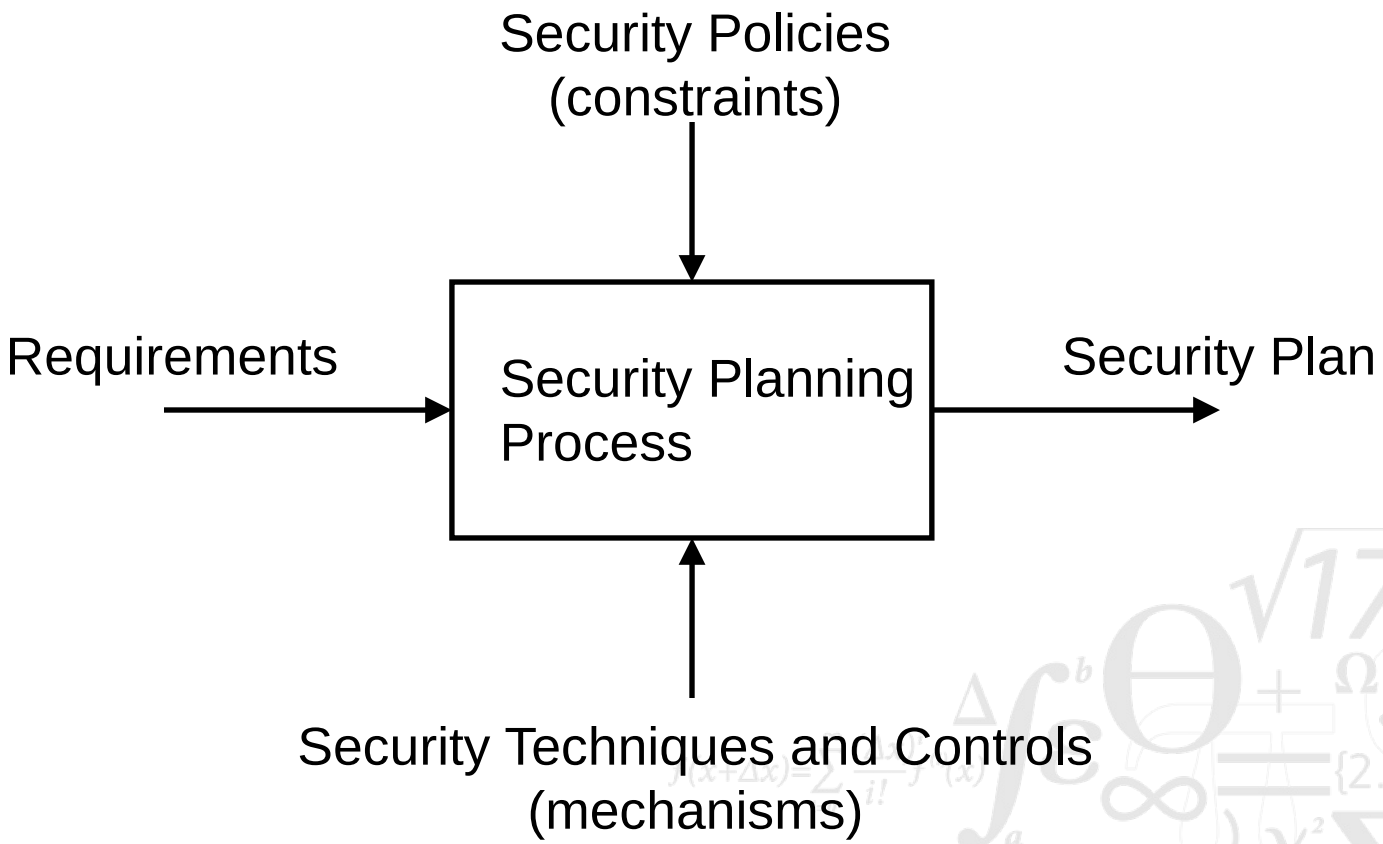


DTU Compute
Department of Applied Mathematics and Computer Science

Four Areas of Security Administration

- Security planning
  - Advance preparation for when things go wrong
  - Define measurable objectives
  - Establish procedures for system evolution
- Security policy definition and enforcement
  - Define goals and ensure that these goals are continuously met
- Physical security
  - Aspects of the physical environment that impact on security
- Risk analysis
  - Analyse threats
  - Weigh cost and benefits of controls

Security Planning Process



Contents of a Security Plan

- **Policy definition:** establish the overall security goals
- **Establish base line:** describe the current state of the system to provide a base line for the work
- **Identify requirements:** identify steps needed to achieve the defined security goals
- **Identify recommended controls:** identify controls to vulnerabilities defined in policy and requirements
- **Establish accountability:** delegate responsibility
- **Define timetable:** define deadlines for phased implementation
- **Show continual vigilance:** define responsibility for maintaining security when system evolves

Defining the Security Policy

- Security policies must have support from the top management
  - Ultimate arbiter in conflicts between security and business goals
  - Ensures buy-in from all levels in the organisation
    - *Requires that CEO walks the talk*

Bank chief quits in sex site scandal

May 30 2004 0:11 AM

JEROME REILLY and DON LAVERY MIKE Soden, the group chief executive of Bank of Ireland, yesterday resigned in disgrace after he admitted accessing adult sex sites on his office computer at the bank's Baggot St headquarters.

Contents of a security Policy

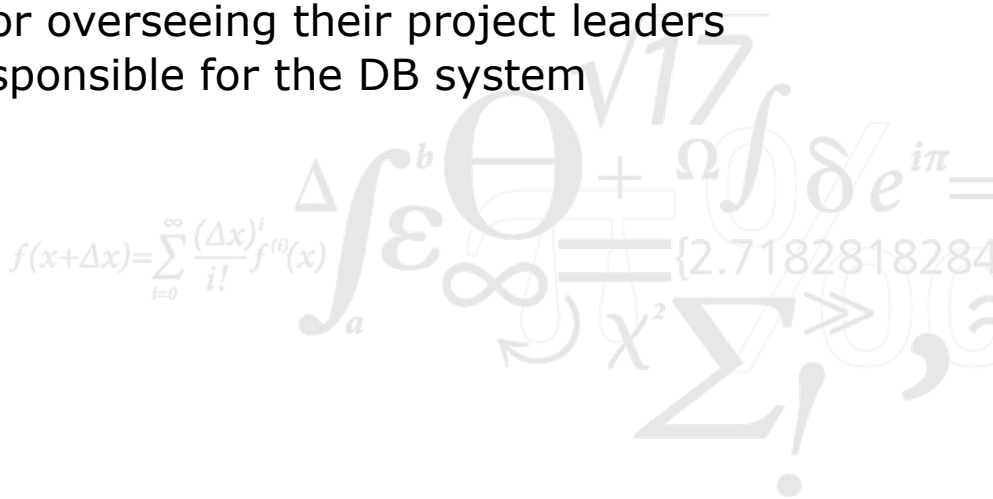
- Security policy should specify:
  - The organizations *goals* for security, e.g., confidentiality, integrity and availability, and their relative importance
  - Responsibility for enforcing security policies
    - *Historically IT Department*
    - *Increasingly responsibility of Finance Department*
    - *Could be placed in a separate Risk Committee, reports to the Board*
  - The organizations commitment to security
- Overall policy must include an access control policy:
  - Who should be allowed access to the system?
  - To what systems and resources should access be allowed?
  - What type of access should be allowed for each resource

Defining the Security Requirements

- The security requirements must address all issues mentioned in the security policy
- Important characteristics:
  - *Correctness:* are requirements understandable and correct?
  - *Consistency:* are there conflicting or ambiguous requirements?
  - *Completeness:* are all possibilities covered?
  - *Realism:* is it possible to achieve the requirements?
  - *Need:* are the requirements unnecessarily restrictive?
  - *Verifiability:* can tests be written to verify that the requirements are met?
  - *Traceability:* can all requirements be traced to the related controls, so that changes in requirements can be easily implemented

Responsibility for Implementation

- Assigning responsibility must also identify coordinators for implementation of the security requirements
  - Who checks for new vulnerabilities
  - Who implements new controls when new vulnerabilities are discovered
- Different responsibilities may be assigned to different groups of users:
  - PC users may be responsible for their own PC
  - Project leaders may be responsible for the data and computers allocated to the project
  - Managers may be responsible for overseeing their project leaders
  - Database administrators are responsible for the DB system



Ensuring commitment to Security Plan

- Acceptance by the organisation is required for the implementation of any security plan
  - Security team must ensure backing from management
  - Security team must be sensitive to the needs of the group affected by the security policy
  - Those affected by the security policy must understand the importance of the imposed controls
    - *This includes running awareness programs*

- Environments change, so security policies must be able to evolve
  - This requires periodic review of security policies, including establishment of a new baseline
  - Evaluation and modification of unfortunate policies

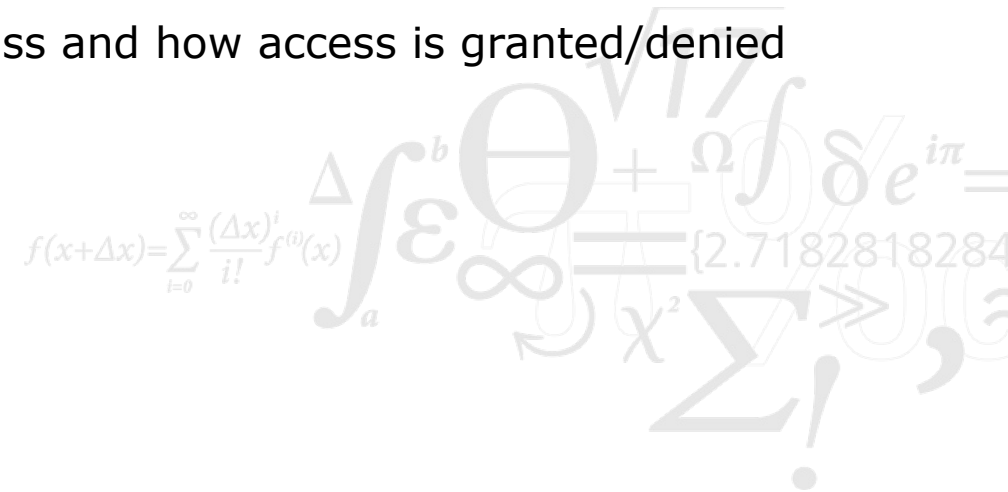
Writing Security Policies

- Security policies are written for several purposes
  - Identify sensitive information assets
  - Clarify security responsibilities
  - Promote awareness for existing employees
  - Guiding new employees

- Security policies have several audiences
  - Users
  - Owners
  - Beneficiaries
  - It is important to balance the interest of all parties

Content of a Security Policy

- State purpose
  - Promote efficient business operation
  - Facilitate sharing of information throughout the organization
  - Safeguard business and personal information
  - Ensure accurate information is available to support business decisions
  - Ensure a safe and productive place to work
  - Comply with applicable laws and regulations
- Protected Resources
  - Explicitly list assets covered by the policy (*which resources*)
- Nature of Protection
  - Indicate *who* should have access and how access is granted/denied



Characteristics of a Good Security Policy

- Coverage
  - The policy should be comprehensive - any incident that may occur should be covered by the policy (make it universal)
- Durability
  - The policy should evolve with the system, but remain largely unchanged (keep it general)
- Realism
  - The policy should not set unobtainable goals or impose unworkable restrictions
- Usefulness
  - The policy should be seen to be useful, otherwise it will be ignored

Physical Security

- Physical security encompass all aspects of security that involve physical controls: walls, locks, guards, emergency generators, fire inhibitors, …

- Physical security should consider:
  - Break-ins, theft, espionage, …
  - Natural disasters
  - Loss of power
  - Loss of communication
  - Human vandals
  - Interception of sensitive information

"Out of Scope" = Somebody Else's Problem

Natural disasters; threats to availability

- Floods
  - Natural floods come from rising water (ground water, rivers)
    - *Flooding is normally slow and some precautions can be made*
  - Sudden floods come from bursting dams, water mains, …
    - *Flooding is difficult to prevent and few precautions can be made*
- Fires
  - Fire is often sudden
    - *Short time to react*
  - Extinguished with water (implies flooding as well)
  - Equipment can be damaged by smoke as well as fire
- Storms, earthquakes, volcanoes
  - Often determined by geographical location

Loss of power and Communications

- Uninterruptible power supply (UPS)
  - Stores energy (battery or wheel) that can be released if the power is cut - normally only allows a clean shutdown
  - UPS can be complemented by a backup generator
- Surge suppressor
  - Some countries have problems with sudden drops, spikes and surges in electrical power, which may damage electrical equipment - surge suppressors limit variations in power
- Multiple ISPs
  - Prevent breakdown if one ISP fails
- Multiple phone lines?
  - In Europe one company (the national PTT) has historically installed the infrastructure and other operators simply lease access to the wire - this is particularly true of the local loop

Dependability of Data Center

Tier	Requirement
I	• Single non-redundant distribution path serving the critical loads • Non-redundant critical capacity components
II	• Meets all Tier I requirements, in addition to: • Redundant critical capacity components • Critical capacity components must be able to be isolated and removed from service while still providing N capacity to the critical loads.
III	• Meets all Tier II requirements in addition to: • Multiple independent distinct distribution paths serving the IT equipment critical loads • All IT equipment must be dual-powered provided with two redundant, distinct UPS feeders. Single-corded IT devices must use a Point of Use Transfer Switch to allow the device to receive power from and select between the two UPS feeders. • Each and every critical capacity component, distribution path and component of any critical system must be able to be fully compatible with the topology of a site's architecture isolated for planned events (replacement, maintenance, or upgrade) while still providing N capacity to the critical loads. • Onsite energy production systems (such as engine generator systems) must not have runtime limitations at the site conditions and design load.
IV	• Meets all Tier III requirements in addition to: • Multiple independent distinct and active distribution paths serving the critical loads • Compartmentalization of critical capacity components and distribution paths • Critical systems must be able to autonomously provide N capacity to the critical loads after any single fault or failure • Continuous Cooling is required for IT and UPS systems.

Human Vandals

- Unauthorised access and use
  - Hire a guard to prevent outsiders from accessing the site
  - Lock servers in rooms that can only be access by authorised personnel
  - Smart cards, RFID or biometrics
- Theft
  - An increasing problem with ubiquitous computing
    - *Example: loss of a MI5 laptop with classified information on it*
    - *Example: DTU requires encrypted hard drives on all laptops*
  - Locks or "screamers" can be used to reduce the risk of theft
  - Smart cards, RFID or biometrics

Interception of sensitive information

- Be careful when disposing of physical media that contains sensitive information
  - A Danish credit information company (RKI) dumped all their paper files in the garbage where journalists got hold of them
  - Recycled hard disks may contain sensitive information
- Shred all paper
  - Especially sensitive information can be burned after shredding
- Overwriting magnetic media
  - Magnetic media retains some magnetisation even after several overwrite - smash media after overwriting
- Degaussing
  - Create a magnetic field that realign magnetic charges
- Emanation protection: Tempest

Awareness & Security Usability

Engagement Survey Invite Inbox x

Qualtrics Team noreply@qualtrics.com via qemailserver.com 2:32 PM (3 minutes ago)

to me

Dear Qualtrics Employee,

The Qualtrics Employee Engagement Survey is designed for you to tell us what we are doing great and what we need to improve. We made great progress because of the feedback that you provided last year. We took action at the company level around compensation, career development, and company transparency to list a few. In addition, each department/region made specific changes to drive improvement.

The survey is completely confidential and we have taken precautions to ensure it stays that way. It won't be possible for any manager to view results for any group of data with less than 5 responses. The anonymity thresholds for comments is set at 25. Please be honest about your experience at Qualtrics.

The survey should take you around 15 minutes to complete, and you have until April 11th to submit your response. If you prefer, you can take the survey at home rather than on company time, and you can access it from any mobile device.

Your link to take the survey is here: Do the Evaluation

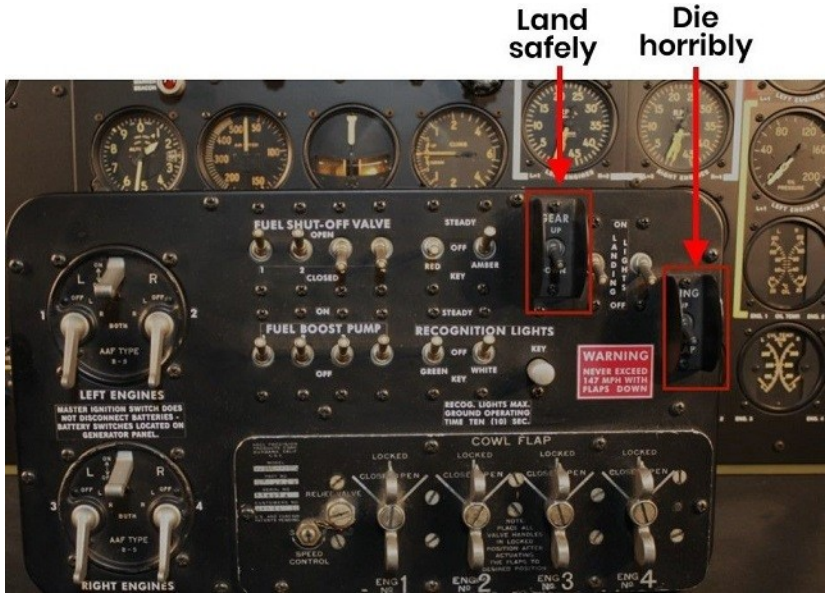
If you have any questions, please contact your survey team at survey@qualtrics.com

Thank you!
Your survey team

Click here to Reply, Reply to all, or Forward

1: https://www2.deloitte.com/my/en/pages/risk/articles/91-percent-of-all-cyber-attacks-begin-with-a-phishing-email-to-an-unexpected-victim.html

Let Form Follow Function



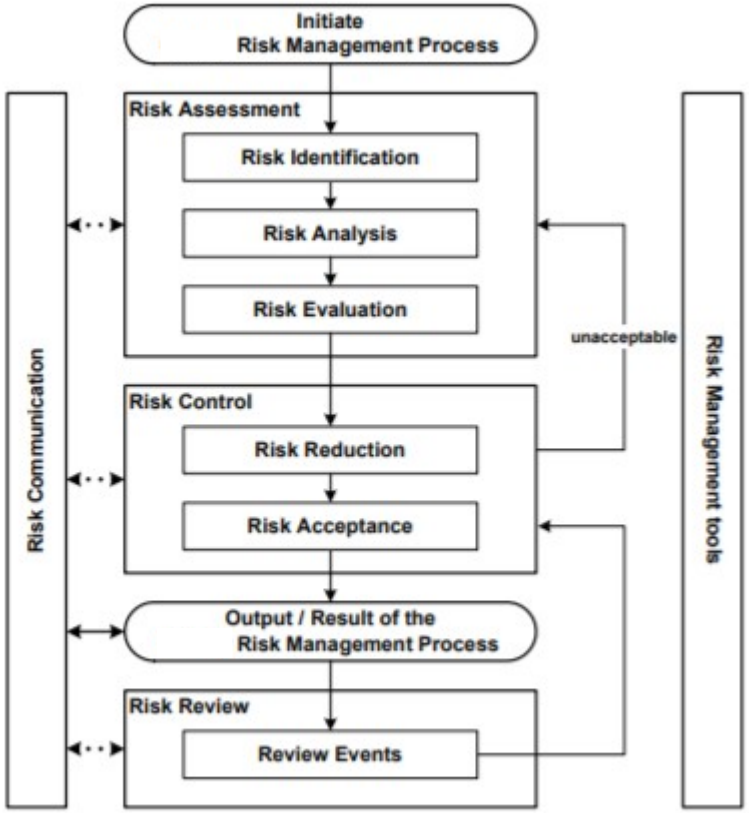
B-17 cockpit instrument panel

Revised levers for landing gear, wing flaps

Pictures from: https://www.ncsc.gov.uk/blog-post/so-long-thanks-for-all-the-bits

Break

Basic Elements of Risk Management



Risk Analysis

- Three elements have to be identified:
  - Loss associated with an event (*risk impact* or *cost*)
  - Likelihood that the event will occur
  - Degree to which we can change the outcome (*risk control*)
    - *By reducing cost or decreasing likelihood of a particular event*
- Exposure associated with a particular event (aka. risk)
  - Cost of event $\times$ likelihood of event
- Three strategies for dealing with risk
  - Avoiding the risk by changing the requirements
  - Transferring the risk, e.g., through insurance
  - Assuming the risk by accepting it; control it with the available resources and accept the loss if the event occurs
- Risk leverage is the relative benefit of reducing risk

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

Difficulty of Measuring Risk

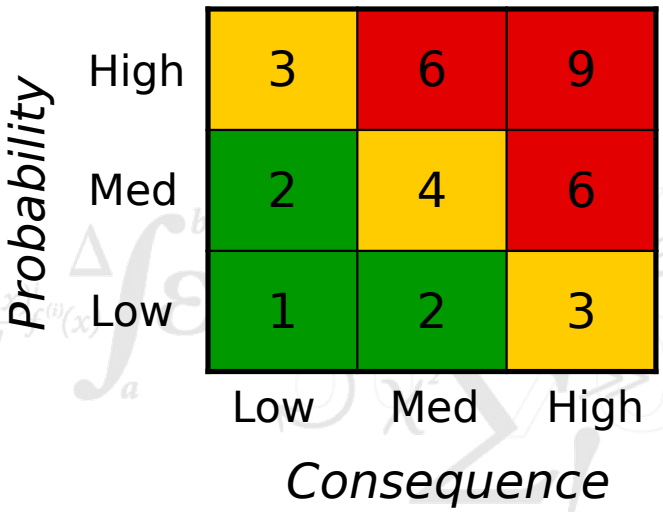
- Estimating likelihood of threats
  - Precise models must include everything
    - *It must effectively describe the whole world*
  - How relevant is past data to the calculation of future probabilities?
    - *The nature of future attacks is unpredictable*
    - *The actions of future attackers are unpredictable*
  - Subjective probabilities look most promising
- Businesses want to measure "costs" in money, but
  - Many assets are difficult to measure in this way
    - *Value of data and in-house software - no market value*
    - *Value of goodwill and customer confidence*
- Measurement of benefit from security measures
  - Problems with the difference of two approximate quantities
    - *How does an extra security measure affect a ~10^{-5} probability of an attack?*

Establish Risk Levels

- Precise monetary values give a false sense of precision
- Better to use levels:
  - High, Medium, Low or Essential-high-medium-low-not important
    - *High: major impact on the organisation*
    - *Medium: noticeable impact ("material" in auditing terms)*
    - *Low: can be absorbed without difficulty*
  - Numerical rating: rating on a scale of 1 – 10
- 3x3 matrix (or 5x5)
  - Commonly used in industry
  - Difficult to decide priority
    - *Is 6 > 6 ?*

Consequence = High, Probability = Med

Consequence = Med, Probability = High



Severity level: CVSS Score

- CVSS Score are a way to provide a qualitative measure of severity **(but not of risk!)** rangin from 0 (lowest) to 10 (highest): https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator
- CVSS 3 consists of three metrics: base, temporal, and environmental
- CVSS 4 consists of four metrics: base, threat, environmental and supplemental
- Vulnerabilities are sorted in 5 categories:
  - None (or informational): 0.0
  - Low: 0.1 – 3.9
  - Medium: 4.0 – 6.9
  - High: 7.0 – 8.9
  - Critical: 9.0 – 10.0

Basic Steps of Risk Analysis

- Identify assets
- Determine possible vulnerabilities
- Estimate likelihood of exploitation
- Compute expected annual loss
- Survey applicable controls and their costs
- Project annual savings of control

Identify Assets

- *Hardware:* computers, peripheral equipment, communication infrastructure
- *Software:* source code, binary programs, operating systems
- *Data:* temporary data, stored data, printed data, backup media
- *People:* skills needed to run systems or programs
- *Documentation:* hardware, software, administrative procedures
- *Supplies:* paper, forms, toner cartridges, magnetic media (including CD-ROMs)

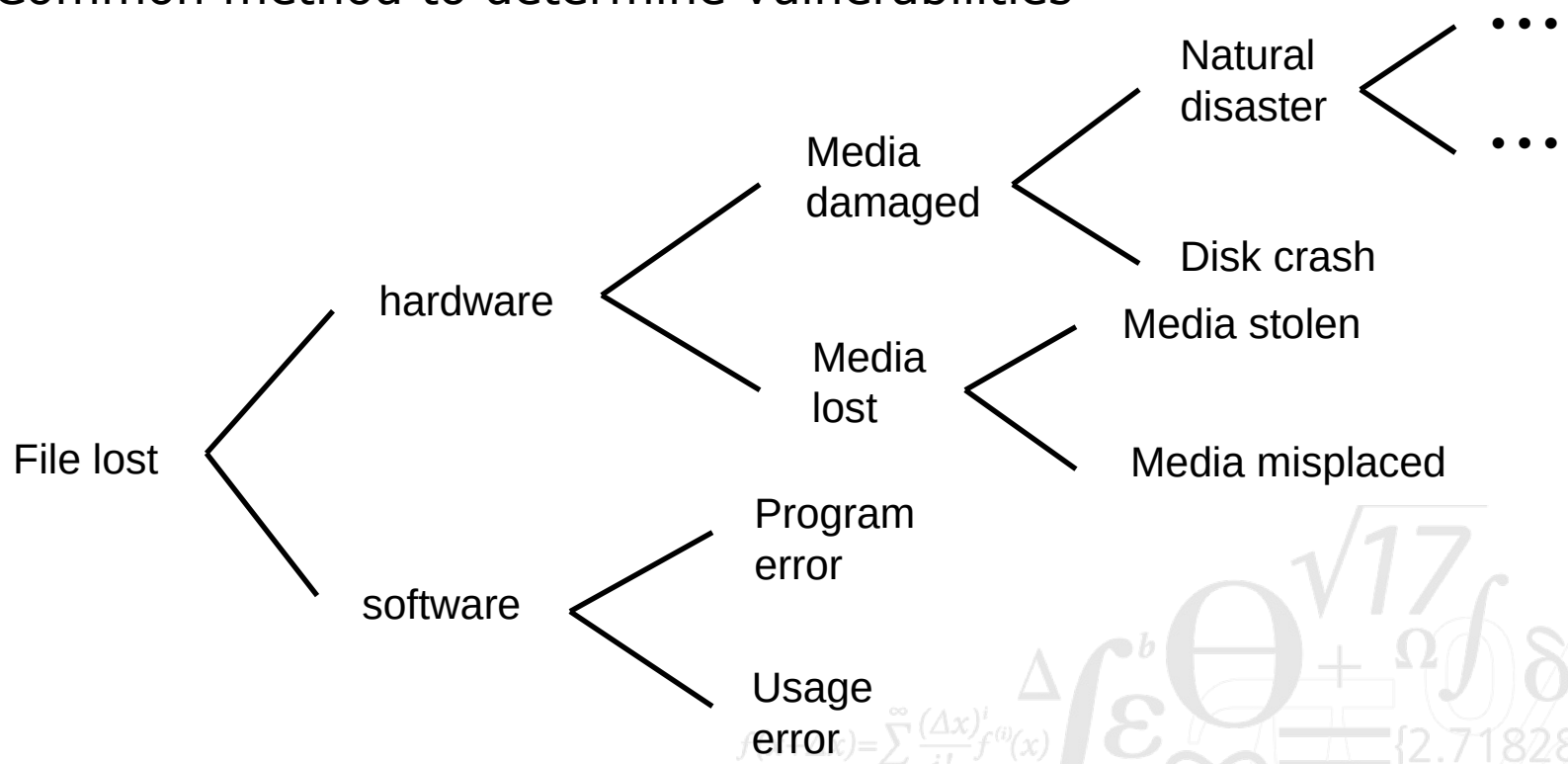
Determine Vulnerabilities

Asset	Confidentiality	Integrity	Availability
Hardware		tampered with	stolen, destroyed
Software	copied, pirated	Trojan horse, backdoor	deleted, license expire
Data	disclosure, inference	damaged	deleted, misplaced
People			quit, retire, vacation
Documentation	copied, stolen	tampered with	lost, stolen, destroyed
Supplies			lost, stolen, damaged

- Fill in the matrix
  - Effects of unintentional errors: typos, insecure disposure of output
  - Effects of malicious insiders: disgruntled employees, bribery, curious browsers (what is the salary of the CEO?)
  - Effects of outsiders: network access, dial-in access, hackers, uninvited visitors, dumpster diving detectives
  - Effects of natural disasters

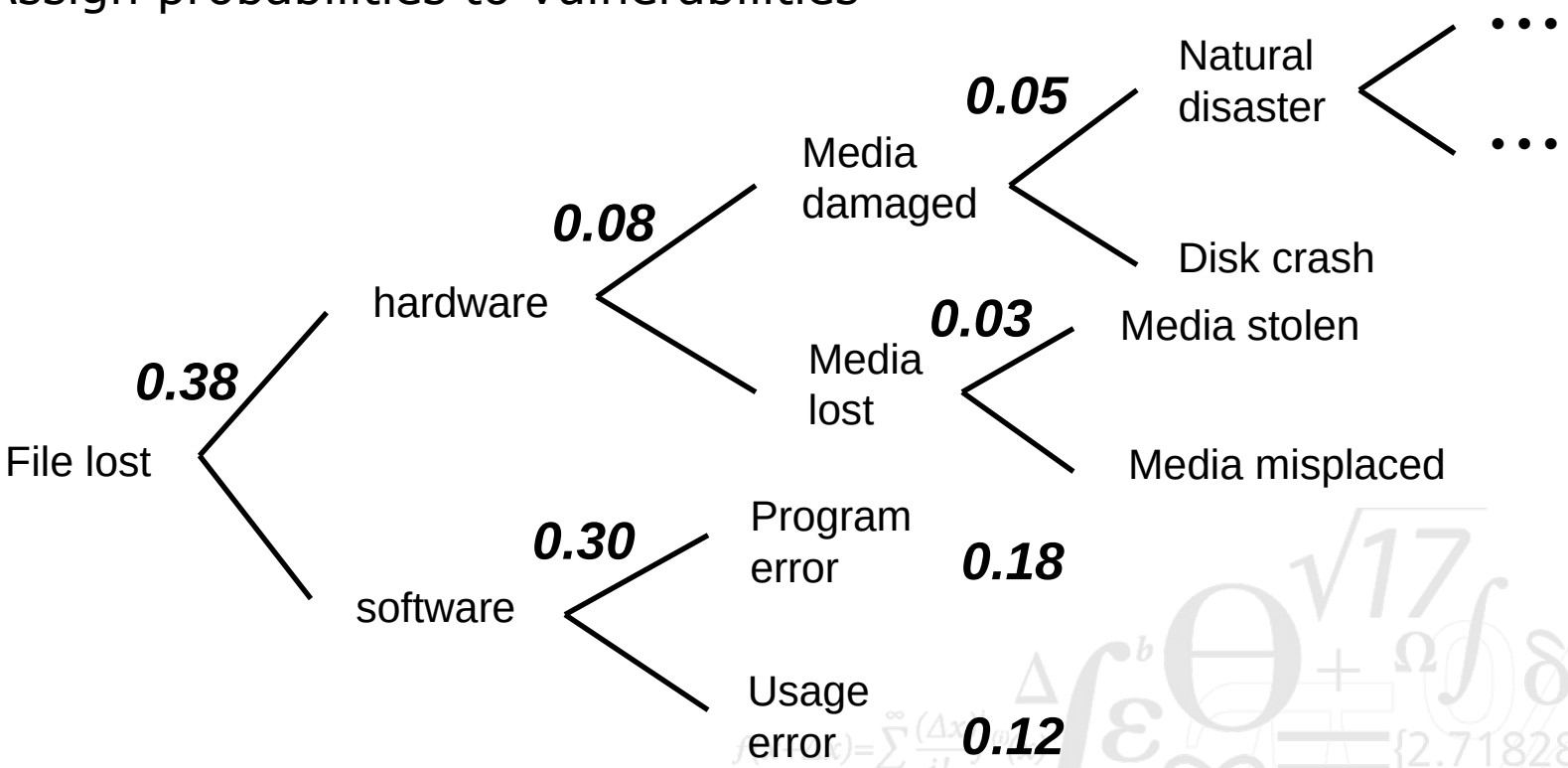
Fault Tree Analysis

- Common method to determine vulnerabilities



Estimate Likelihood of Exploitation

- Assign probabilities to vulnerabilities



Compute Expected Annual Loss

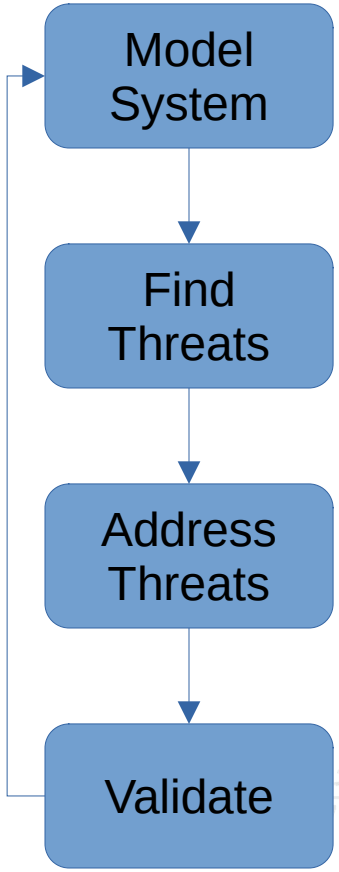
- Not all risks are equally severe
  - Safety critical: human lives are at stake
  - Mission critical: survival of the company is at stake
  - Costly: major impact on the earnings of the company
  - Negligible: costs are small compared with operational costs
- Knowing probability and cost of the event allows computation of the expected annual loss
- *Example: Credit card companies accept a certain amount of fraud*

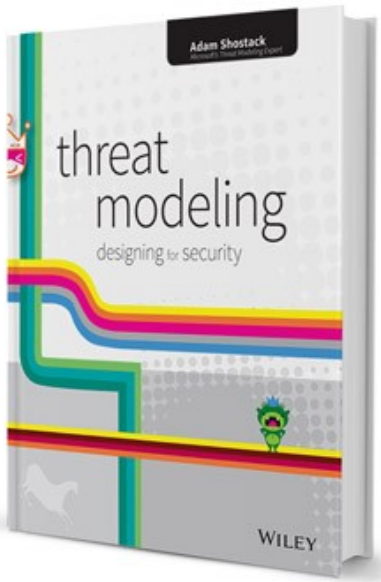
Measure All Costs

- Hidden costs are easy to forget:
  - Unavailability of the system, restore data from backups, reinstallation of software
- Consider the following questions:
  - What legal obligations exist for confidentiality and integrity of data
  - What contractual obligations may be applicable (*fines?*)
  - Could release of data harm individuals or organizations
    - *Will they litigate?*
  - Could event cause missed business in the future
  - What are the psychological effects of event
    - *Embarrassment, loss of credibility, loss of business, …*
  - What is the value of access to data (worth a backup site)
  - What other problems could arise from loss of data
    - *Can data be restored*

Know your system, a.k.a Threat Modelling

- The Four-Step Framework
  - What is your system?
  - What can go wrong with it?
  - What should you do about those things that can go wrong?
  - Was your analysis correct/good enough?

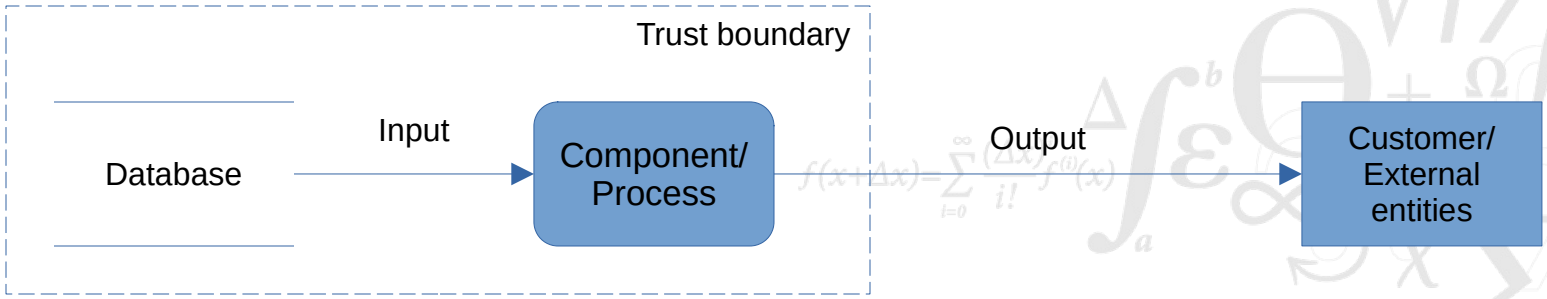




Adam Shostack, Threat Modeling: Designing for Security: https://shostack.org/books/threat-modeling-book

What is your system, a.k.a information gathering

- Information gathering
  - List the different components and/or processes of the system
  - List the different data stores
  - List the external entities that communicate with the system and draw the trust boundaries
  - List the interactions between these elements



Data-Flow Diagram (DFD)

Find Threats

What can go wrong with it

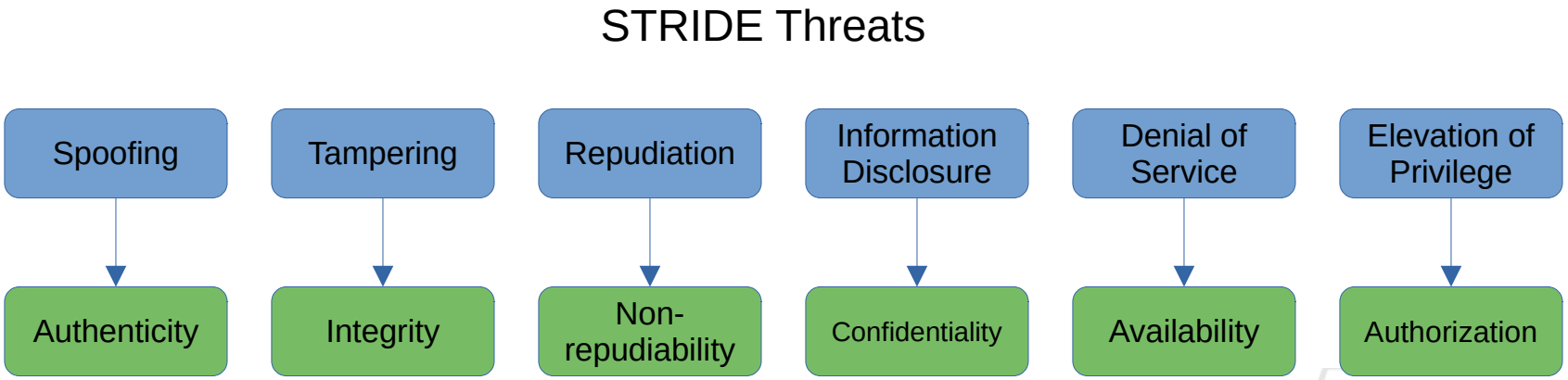
STRIDE Threats

Spoofing | Tampering | Repudiation | Information Disclosure | Denial of Service | Elevation of Privilege

- The STRIDE framework was first introduced by Loren Kohnfelder and Praerit Garg in 1999: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN
- **Spoofing**: pretending to be something or someone other than yourself
- **Tampering**: modifying something on disk, on a network or in memory
- **Repudation**: claiming that you did not do something, or were not responsible
- **Information Disclosure**: providing information to someone not authorized to see it
- **Denial of service**: absorbing resources needed to provide service
- **Elevation of Privilege**: allowing someone to do something they are not authorised to do

Address Threats

What should you do, a.k.a mitigations



Validate

What can go wrong with it

STRIDE Threats

Spoofing	Tampering	Repudiation	Information Disclosure	Denial of Service	Elevation of Privilege

- Test the mitigations (pentest, code reviews, etc.) as mitigations can also introduce new threats
- Confront the threat modelling with different group of stakeholders (developers, architect, owners, CISO, etc.)
- Use the feedback to update and repeat the process (this is a continuous process)

Management Frameworks and Governance Structures

- A number of standards and best practices are commonly used

- ISO 27000 series
  - Family of standards on Information Security Management Systems
  - *Available as "Dansk Standard" through the DTU Library*
- NIST Special Publication 800 series
  - NIST SP 800-39
  - NIST Cybersecurity Framework
  - *All publications available online at NIST*
- CIS Critical Security Controls
  - CIS defines a number of controls too improve security
  - Latest version is CIS v8 (earlier version is known as CIS20)
  - *Available at: https://www.cisecurity.org/controls/v8/*

GRC – Governance, Risk, Compliance