Browser Attacks

Man-in-the-Browser (MitB): This is a stealthy attack where malware, often delivered through a trojan, infects a web browser and intercepts communications between the user and the web application. It can modify web pages and steal sensitive information like login credentials or financial data without the user's knowledge, even if the site uses HTTPS.

Keystroke Logger: A keystroke logger (or keylogger) is a type of spyware that records every keystroke made by a user on their keyboard. It can be used to capture sensitive information such as passwords, credit card numbers, and personal messages. Keyloggers can be either hardware or software-based and often operate without detection.

Page-in-the-Middle: This attack involves intercepting a user's web request and serving them a fake but convincing replica of a legitimate website. The goal is usually to trick users into entering sensitive information, which the attacker then captures. It's a form of phishing that relies on web spoofing and is often executed via DNS hijacking or malicious proxy servers.

Program Download Substitution: In this attack, a legitimate software download is intercepted and replaced with a malicious version. This can occur through compromised websites, man-in-the-middle attacks, or malicious download links. Once the user installs the fake program, the attacker gains access to the system or data.

User-in-the-Middle: This term refers to scenarios where an attacker tricks or manipulates a legitimate user into unknowingly assisting with an attack. For example, a user might be lured into clicking a malicious link or entering credentials into a fake login page. Unlike typical "man-in-the-middle" attacks, this approach leverages social engineering and human error.

These attacks are largely due to failures of authentication. They can be prevented by:

Shared Secret: A shared secret is a piece of information known only to the user and the authenticating server (like a PIN, password, or cryptographic key). If properly implemented and not exposed to malware or intercepted, it can prevent unauthorized access. For example, even if a keystroke logger captures credentials, additional verification based on a shared secret (e.g., answering a security question) can stop an attacker from gaining full access.

One-Time Password (OTP): OTPs are temporary and unique codes that expire quickly, typically used in two-factor authentication (2FA). They render many attacks useless — for instance, if a **Man-in-the-Browser** or **Page-in-the-Middle** attack captures an OTP, it cannot be reused after it expires. This greatly limits the attack window and increases the security of the authentication process.

Out-of-Band Communication: This involves using a separate channel (like SMS, email, or a phone call) to verify identity or confirm actions. It helps mitigate attacks like **Program Download Substitution** or **User-in-the-Middle** by requiring user confirmation from a different device or medium, which an attacker typically cannot intercept if they only have access to the primary channel. For example, if a user tries to log in from a suspicious IP, they might receive a verification code on their phone, adding a strong layer of defense.

Some more attacks:

Tracking Bug: A small, invisible image or script embedded in emails or web pages to secretly track user activity. It collects data like IP address, time opened, and user behavior.

Clickjacking: Tricks users into clicking something different from what they perceive, like a hidden button or link. This can lead to unintended actions like changing settings or authorizing transactions.

Drive-by Download: Malware is automatically downloaded and installed without the user’s knowledge when they visit a compromised or malicious site. No interaction is needed from the user.

XSS (Cross-Site Scripting): Injects malicious scripts into trusted websites, which then run in the browsers of users who visit. This can steal cookies, session tokens, or manipulate page content.

SQL Injection: Attackers insert malicious SQL queries into input fields to access, modify, or delete data from a database. Poor input validation makes applications vulnerable to this.

Dot Dot Slash (../) Attack: Also known as directory traversal, it exploits file path input to access files outside the intended directory. It can expose sensitive system files or application data.

SSI (Server Side Includes) Injection: Injects malicious SSI commands into web pages processed by the server. If executed, it can run arbitrary commands or reveal internal server data.

Injection based attacks can be countered by the following steps:

- Filter and sanitize all user input
- Need to account for every potentially valid encoding

- Make no assumptions about the range of possible user inputs—trust nothing, check everything
- Use access control mechanisms on backend servers, such as “stored procedures”

Phishing

Phishing is a cyberattack where criminals try to steal personal or financial information or install malware by tricking users into clicking malicious links or revealing sensitive data. These attacks often come via emails or fake websites that appear to be from trusted companies, organizations, or individuals. Phishing campaigns frequently exploit timely events like natural disasters, epidemics, or political events to seem more convincing.

Types of Phishing

- **Mass Phishing**
  - Broad, high-volume emails sent to many recipients.
  - Generic and not personalized.
- **Spear Phishing**
  - Targeted at specific individuals or organizations.
  - Personalized using details about the victim.
- **Whaling**
  - Focuses on high-profile targets (e.g., executives).
  - Seeks access to sensitive or high-value information.
- **Clone Phishing**
  - Copy of a legitimate, previously sent email.
  - Malicious links/attachments replace the original ones.
- **Advance-Fee Scam**
  - Victim is promised a reward in exchange for an upfront payment.
  - Often asks for bank details or money transfer.

Spear Phishing

Spear phishing is a targeted cyberattack where attackers craft convincing, personalized emails to deceive specific individuals, often high-level employees like CFOs or directors. Unlike mass phishing, spear phishing uses detailed information—often gathered from social networks—to trick recipients into clicking malicious links or opening infected attachments. This allows attackers to bypass traditional security defenses and gain a foothold in the organization's network.

These attacks are particularly dangerous because they are hard to detect and highly effective. Spear phishing is often used to deploy ransomware, steal sensitive data, or gain long-term access to internal systems. The personalized nature of these emails can fool even experienced professionals, making them a preferred method for cybercriminals. In fact, 84% of organizations reported falling victim to successful spear phishing attacks in 2015.

Characteristics of spear phishing:

Blended or Multi-Vector Threat: Combines email spoofing, dynamic URLs, and drive-by downloads to bypass defenses.
Use of Zero-Day Vulnerabilities: Targets unpatched flaws in browsers and applications to exploit systems.
Multi-Stage Attack: Begins with system compromise, followed by malware, data exfiltration, and further attacks.
Well-Crafted Email Forgeries: Personalized emails that evade traditional spam filters and reputation checks.

Some baiting tactics:

- Notification from a help desk or system administrator
- Advertisement for immediate weight loss, hair growth or fitness prowess
- Attachment labeled "invoice" or "shipping order"
- Notification from what appears to be a credit card company
- Fake account on a social media site

Preventing Phishing:

Check for Errors: Look for spelling, punctuation mistakes, or poor grammar.
Verify URLs: Hover over links to check if the hyperlinked URL differs from the displayed one.
Threatening Language: Beware of urgent messages demanding immediate action.
Install Antivirus: Keep antivirus software updated on all devices.
Use Email Filters: Filter out spam and malicious traffic.
Avoid Giving Personal Info: Legitimate businesses never ask for passwords via email.
Don't Send Private Info by Email: Never share passwords or bank details via email; verify requests through other means.

DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email security standard that:

- Confirms the sender’s identity using **Sender Policy Framework (SPF)** and **DomainKeys Identified Mail (DKIM)**.
- Instructs the recipient’s email service on how to handle emails that fail authentication checks.
- Requests recipient email services to send reports on email origin and usage.

Benefits of DMARC:

- **Protects Users and Reputation**: Shields users, employees, and brand reputation from cybercrime.
- **Reduces Support Costs**: Lowers customer support costs related to email fraud.
- **Improves Trust**: Enhances trust in legitimate emails sent by your organization.
- **Visibility**: Provides insights into both legitimate and fraudulent use of your domain through DMARC reports.

Security Incident Management

Contents of a Security Plan

- Policy: The goals of the computer security effort and the willingness of the people involved to achieve those goals
- Current State: The status of security at the time of the plan
- Requirements: Recommending ways to meet security goals
- Recommended Controls: Mapping controls to vulnerabilities and requirements of the plan
- Accountability: Documenting who is responsible for each security activity
- Timetable: Identify when each security function is to be done
- Maintenance: Specifying a method for periodically updating the plan

Policy:

High level statement of purpose or intent of the security plan. It should answer three questions,

1. Who should be allowed access
2. Which resources should access be allowed to
3. Which users should be allowed to access which resources

The policy should specify the organisation's security goals, where the responsibility of security lies and the organisation's commitment to security.

Assessment of Current Security State:

A risk analysis is carried out which is a systematic investigation of the system, its environment and vulnerabilities and what might go wrong. This describes the present state of the security before implementation of the plan.

It defines the limit of responsibility for security, i.e.

1. Which assets are to be protected
2. Who is responsible for protecting them
3. Who is excluded from responsibility

Requirements of Security

Security requirements are functional or performance demands that are placed on a system to ensure a desired level of security, derived from business needs and compliance to government standards.

Characteristics of good security requirements:

Correctness: Are requirements understandable and without error?
Consistency: Are there any conflicting or ambiguous requirements?
Completeness: Are all possible scenarios addressed?
Realism: Is it possible to realistically implement what the plan mandates?
Need: Are the requirements unnecessarily restrictive?
Verifiability: Can we test that the requirement has been met?
Traceability: Can the requirements be traced back to functions and data making changes and maintenance easy?

Responsibility for Implementation

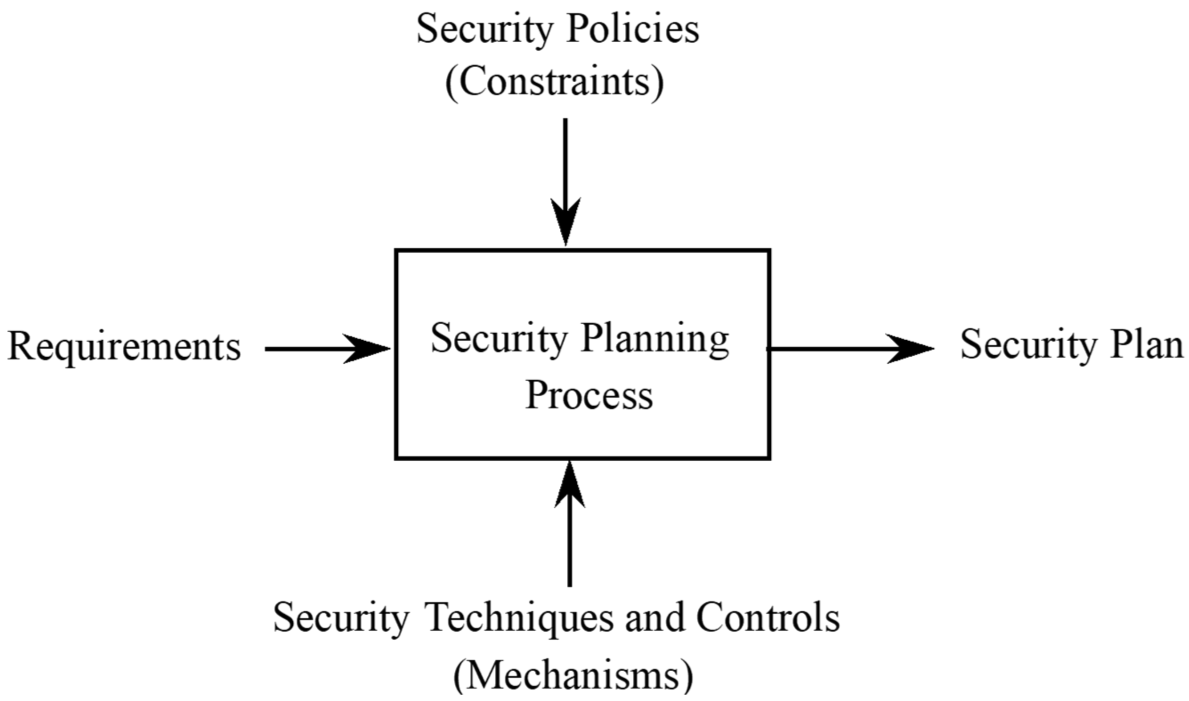
A section of the security plan will identify which people (roles) are responsible for implementing security requirements.

Common roles:
Users of personal computers or other devices may be responsible for the security of their own machines. Alternatively, the security plan may designate one person or group to be coordinator of personal computer security.
Project leaders may be responsible for the security of data and computations.
Managers may be responsible for seeing that the people they supervise implement security measures.
Database administrators may be responsible for the access to and integrity of data in their databases

Timetable and Plan Maintenance

The Security Plan should also outline how and when each element of the plan will be implemented and performed. It should order the elements of the plan from most to least important so the biggest vulnerabilities can be dealt with first.

There should also be considerations made for the plan to be extensible as new equipment will be obtained and new threats should emerge. It should also include a schedule for periodic review and maintenance.



Members of the Security Plan

- Computer hardware group
- System administrators
- Systems programmers
- Applications programmers
- Data entry personnel
- Physical security personnel
- Representative users

Success of the security plan depends on the commitment of three groups of people to follow the plan:

- The designers of the plan should be sensitive to the people the plan affects
- Those affected by the plan should know how the plan affects how they use the system
- The management should be committed to using and enforcing use of the security plan

Business Continuity Planning

A business continuity plan documents how the business will continue to function in the event of a security incident and after it.
It addresses situations having two characteristics:

- Catastrophic situations, where all or major part of computing capability is suddenly unavailable
- Long duration, in which the outage is expected to last so long that the business will suffer

Activities:

- Assesses the business impact of the crisis - What are the most important assets and what will affect it
- Develop a strategy to control impact and safeguard key assets
- Develop and implement a plan for the strategy i.e who is in charge, who performs what tasks when an incident occurs

Incident Response Plan

An incident response plan tells the staff how to deal with a security incident. While a business continuity plan worries about business issues, the incident response plan focuses on how to deal with the current security issues.
The plan should define

1. What constitutes an incident
2. Who should take charge
3. Describe the plan of action

CSIRT (Computer Security Incident Response Team)

They are teams trained and authorized to handle security incidents.

Responsibilities:

- Reporting: Receive information on and report to senior management about security issues
- Detection: Investigate to see if incident has occured
- Triage: take immediate action to address urgent needs
- Response: Coordinate effort and respond appropriately to the incident
- Postmortem: Declare the incident over and analyse it to improve future responses
- Education: Prevent incidents by advising on good security practices

Skills:

- Collect and analyse forensic evidence
- Analyse data and infer trends
- Analyse source and impact of malicious code
- Perform penetration testing and vulnerability analysis
- Understand current technologies used in attacks

Risk Analysis

A risk is a potential problem the system or its users may experience.

Risk Analysis is an organised process for 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.

Characteristics of a risk:
Probability it occurs
Impact or damage caused
Degree to which we can change the outcome

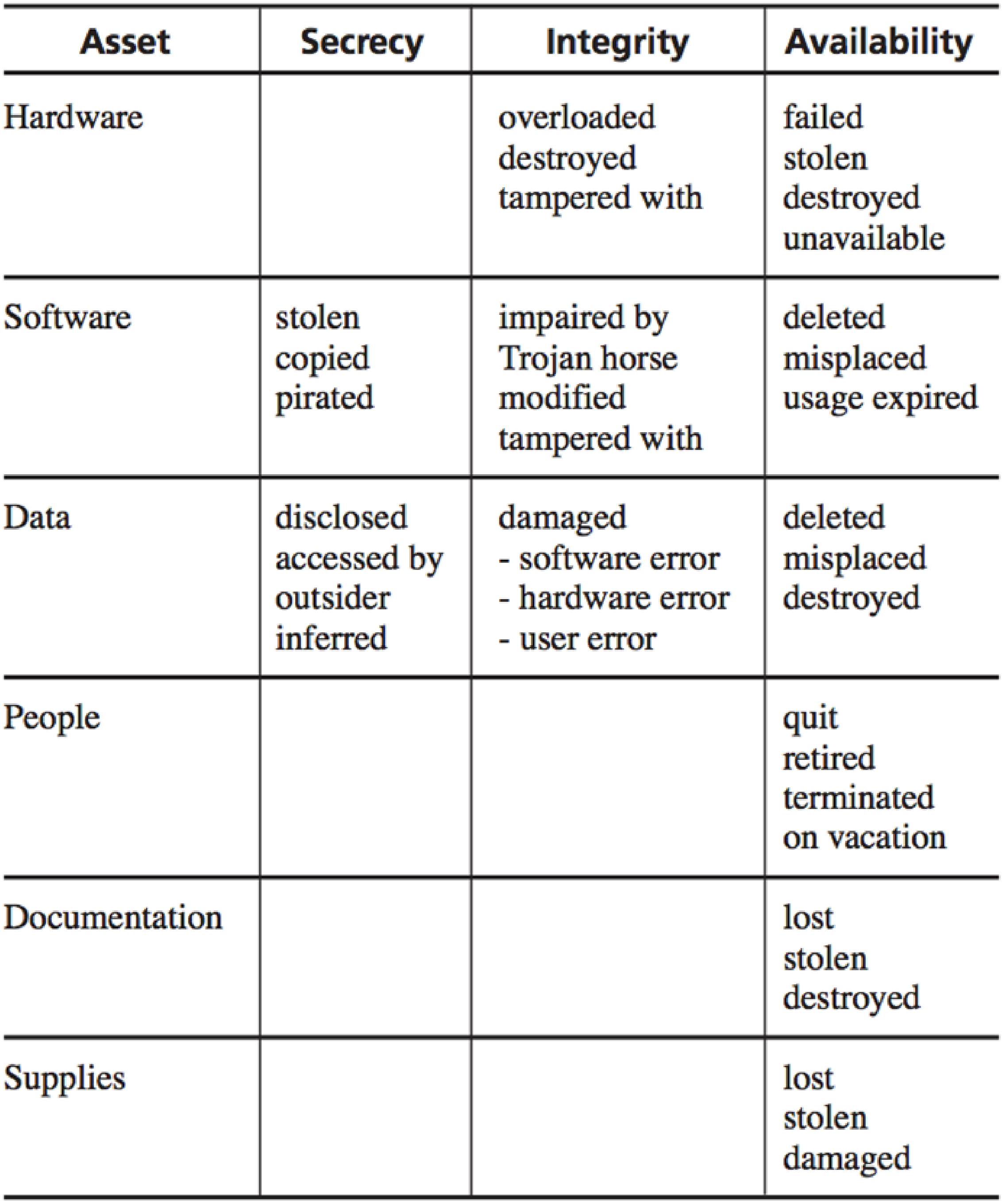
Risk Management Strategies

Avoid the risk by changing requirements of the security plan or modifying the system
Transfer the risk by allocating it to other systems people or organisations or buying insurance
Assume the risk by accepting it, controlling it, preparing to deal with the loss if it occurs

Steps of Risk Analysis

1. **Identify Assets**
   Hardware, Software, Data, Supplies, Reputation, etc. (give examples of each)

2. **Determine Vulnerabilities**



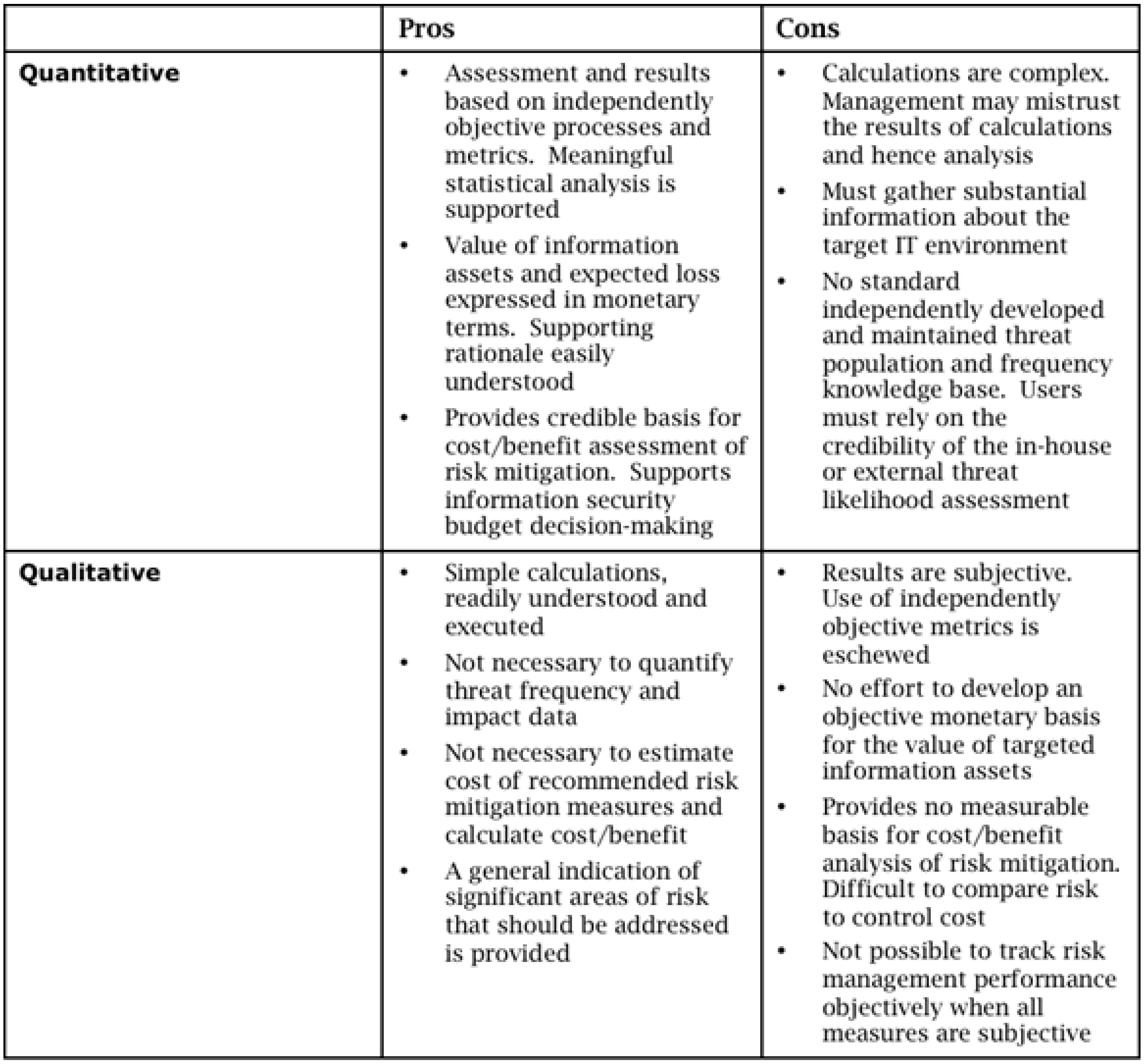
Asset	Secrecy	Integrity	Availability
Hardware		overloaded destroyed tampered with	failed stolen destroyed unavailable
Software	stolen copied pirated	impaired by Trojan horse modified tampered with	deleted misplaced usage expired
Data	disclosed accessed by outsider inferred	damaged - software error -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

3. Estimate likelihood of exploitation

It is impossible to accurately predict the likelihood of exploitation as we do not know all of the systems vulnerabilities.

Some approaches to estimation are:

- Use probabilities from a similar system
- Use a simple rating system
- Use Delphi method



	Pros	Cons
Quantitative	• Assessment and results based on independently objective processes and metrics. Meaningful statistical analysis is supported • Value of information assets and expected loss expressed in monetary terms. Supporting rationale easily understood • Provides credible basis for cost/benefit assessment of risk mitigation. Supports information security budget decision-making	• Calculations are complex. Management may mistrust the results of calculations and hence analysis • Must gather substantial information about the target IT environment • No standard independently developed and maintained threat population and frequency knowledge base. Users must rely on the credibility of the in-house or external threat likelihood assessment
Qualitative	• Simple calculations, readily understood and executed • Not necessary to quantify threat frequency and impact data • Not necessary to estimate cost of recommended risk mitigation measures and calculate cost/benefit • A general indication of significant areas of risk that should be addressed is provided	• Results are subjective. Use of independently objective metrics is eschewed • No effort to develop an objective monetary basis for the value of targeted information assets • Provides no measurable basis for cost/benefit analysis of risk mitigation. Difficult to compare risk to control cost • Not possible to track risk management performance objectively when all measures are subjective

-

4. 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

5. Survey applicable controls and their costs

Once we have all the data regarding vulnerabilities, estimated likelihood, expected loss, etc, we can select the control measure we want to use. Each vulnerability may have more than one control associated with it. One approach is to use graph theory to select a minimal set of controls to address all vulnerabilities

6. Project annual savings of control

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

Arguments for Risk Analysis

- Improve awareness
- Relate security mission to management objectives
- Identify assets, vulnerabilities, and controls
- Improve basis for decisions
- Justify expenditures for security

Arguments Against Risk Analysis

- False sense of precision and confidence
- Hard to perform
- Immutability
- Lack of accuracy

OWASP

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications and APIs that can be trusted.

OWASP Top Ten 2017
A1 Injection
A2 Broken Authentication
A3 Sensitive Data Exposure
A4 XML External Entities (XXE)
A5 Broken Access Control
A6 Security Misconfiguration
A7 Cross-Site Scripting (XSS)
A8 Insecure Deserialization
A9 Using Components with Known Vulnerabilities
A10 Insufficient Logging & Monitoring

Read this once
https://docs.google.com/presentation/d/1VVU61V-GWpFYJhvZQVwbuGcUg2WNuPXe/edit?usp=sharing&ouid=101863828609993646991&rtpof=true&sd=true

They could ask a bit about the 10 attacks.