



EBU5608 Product Development and Management

Topic 19 – Cybersecurity and Managing Risks

Agenda

- The scope and objectives of cybersecurity
- Trends and drivers of cybersecurity
- Key concepts
- Risk management



The big questions is..

Why do you think engineers need to know about
cybersecurity?

What is Cybersecurity?

- Cybersecurity is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks
- It aims to reduce the risk of cyber attacks, and protect against the unauthorised exploitation of systems, networks and technologies
- Increasingly implemented through laws and regulations
- Three distinct legal elements: information security, privacy and data protection, and cybercrime

Information Security

- Seeks to protect all information assets, whether in hard copy or in digital form
- Information is one of the most valuable assets
- Good business practice
- Digital revolution changed how people communicate and conduct business
- New possibilities & challenges

Privacy and Data Protection

- Number of different, but related concepts
- Control of personal data
- Control = the ability to specify the collection, use, and sharing of their data
- Personal information – private x publicly available
- **Data privacy** are the regulations, or policies, that governs the use of my data when shared with any entity, while **data protection** is the mechanism — that is, the tools and procedures — to enforce the policy and regulation, including the prevention of unauthorized access or misuse of the data that I agreed to share

Information Security x Privacy

- Information security and privacy are closely related, but distinct concepts
- Privacy is an individual's right to control the use and disclosure of their own personal information
- Information security is the process used to keep data private
- Security is the process; privacy is the result

Cybercrime


- Cybercrime is an act that violates the law, by using information and communication technology (ICT) to either target networks, systems, data, websites and/or technology or facilitate a crime
- Cybercrime knows no physical or geographic boundaries and can be conducted with less effort, greater ease, and at greater speed and scale than traditional crime

Drivers of Cybersecurity


- Legal and regulatory
 - Growing legal framework establishing safeguarding and information obligation
 - Growing enforcement as a response to ineffective self-regulation
- Commercial
 - Growing awareness of risk, economic and legal consequences, trustworthiness of business transactions
- Technical
 - With technological innovation comes opportunities as well as risks

Information Security I

- Processes, procedures and infrastructure to preserve:
 - confidentiality
 - integrity, and
 - availability of information



Information Security II



11

Confidentiality I

- Confidentiality means that only people with the right permission can access and use information
- Protecting information from unauthorised access at all stages of its life cycle
- Information must be created, used, stored, transmitted, and destroyed in ways that protect its confidentiality

Confidentiality II

- Ensuring confidentiality – encryption, access controls
- Compromising confidentiality – (intentional) shoulder surfing, social engineering; (accidental) publication
- It may result in identity theft, threats to public safety

Example

In 2017, a memory stick with confidential Heathrow airport security files was found in the street – posing a risk to national security. The USB stick was found by a member of the public. It contained information such as: the exact route the Queen takes when using the airport and security measures used to protect her; files disclosing every type of ID needed – even those used by covert cops – to access restricted areas; or a timetable of patrols that was used to guard the site against suicide bombers and terror attacks.

Certain aspects of this information may make it easier for potential attackers to avoid detection. And the cumulative impact of having so many documents, videos, maps and images all in one place represents a security risk.

Integrity

- Integrity means that information systems and their data are accurate
- Changes cannot be made to data without appropriate permissions
- Ensuring integrity – controls ensuring the correct entry of information, authorization, antivirus
- Compromising integrity – (intentional) employee or external attacks; (accidental) employee error

Example

A malicious data breach carried out by a disgruntled employee harm both confidentiality and integrity.

In 2014, Morrisons, the fourth largest supermarket chain in the UK, suffered a serious data breach when the payroll data of nearly 100,000 employees (including names, addresses, dates of birth, national insurance numbers and bank details) were posted online.

A senior IT auditor, Andrew Skelton, posted the payroll data online on a public file-sharing website, tipping off the press and attempting to implicate an innocent colleague.

Skelton was jailed for eight years after being found guilty at Bradford Crown Court of fraud, securing unauthorised access to computer material and disclosing personal data.

Authentication

- Specific to integrity and confidentiality considerations
- Authentication is the process of validating the identity of a registered user or process before enabling access to protected networks and systems.
- Analogue
 - signatures, handwriting, in person attestation, witnesses, notary
- Digital
 - username and password, digital signatures, fingerprints or face recognition

Availability

- Availability is the security goal of making sure information systems are reliable
- Data is accessible
- Individuals with proper permission can use systems and retrieve data in a dependable and timely manner
- Ensuring availability – recovery plans, backup systems
- Compromising availability – (intentional) denial of service (DoS) attack, (accidental) outage

Example

In 2017, WannaCry malicious software has hit Britain's National Health Service, some of Spain's largest companies including Telefónica, as well as other computers across the world, leading to PCs and data being locked up and held for ransom.

The ransomware uses a vulnerability first revealed to the public as part of a leaked stash of NSA-related documents in order to infect Windows PCs and encrypt their contents, before demanding payments of hundreds of dollars for the key to decrypt files. Ransomware is a particularly nasty type of malware that blocks access to a computer or its data and demands money to release it.

Information Security

= Mitigating risks to the trustworthiness of information of corporations and governments by the:

- Development of strategies and
- Implementation to technologies and procedures in order to preserve its
 - confidentiality,
 - integrity, and
 - availability

appropriate to the time and circumstances

Information Security Key Concepts

- Risk management as means to justify information security laws
 - = process of listing the all the relevant factors and taking steps to control them where possible
- There are four main concepts:
 - Vulnerabilities
 - Threats
 - Risks
 - Safeguards

Vulnerabilities I

= weakness or flaw in the information system that can be exploited

- Construction, design mistake
- Flaws in how internal safeguards are used/not used, based on:
 1. People
 2. Process
 3. Facility
 4. Technology

Vulnerabilities II

- People
 - separation of duties principle
 - two or more people need to split a critical task functions
 - Process
 - flaws in organization's procedures
 - missing step in a checklist /no checklist
 - failure to apply hardware and software patches
- = patch is a software/code that updates a program to address security problems

Vulnerabilities III

- Facility
 - flaws in physical infrastructure
 - fences, locks, CCTV cameras
- Technology
 - design flaws
 - unpatched applications, improperly configured equipment
- Successful attacks take place when vulnerability is exploited

Threats I

= anything that can cause harm to an information system – successful exploits of vulnerabilities

- Relationship between a vulnerability and a threat
 - An organization does not have sufficient controls to prevent an employee from deleting critical computer files (**lack of controls – vulnerability**). An employee could delete files by mistake (**employee – source of threat**) (**deleting critical files – threat**). If the files are deleted, successful exploit of the vulnerability has taken place. If the file is not recoverable, the incident harms the organizations and its security. **Availability is compromised**.

Threats II

1. Human
 - Internal and external, includes well-meaning employees and external attackers
2. Natural
 - uncontrollable events (fire, flood)
3. Technology and operational
 - operate inside information systems (malicious code, hardware and software failures)
4. Physical and environmental – lack of physical security
 - Accidental or intentional
 - Internal or external attackers

Threats III

- Threats to information, networks, systems have increased
 - More devices, more use, more 'always on'
 - More complex networks with greater 'attack surface'
 - Bring your own device (BYOD) means that end points of corporate networks no longer in their control; more points of entry into enterprise networks
 - More devices with IoT; smart watches possibly not connected to enterprise authentication systems
- Attacks have grown more sophisticated
 - Sony's servers wiped after internal communications stolen, but held for months
 - Attacks that take months to achieve goals; undetected
 - 'Ransomware' = threat to encrypt data unless paid
 - SolarWind cyberattack

Risks I

= a likelihood that a threat will exploit a vulnerability and cause harm, where the harm is the impact to organization

$$\textit{Risk} = \textit{vulnerability} + \textit{threat}$$

Risk II

- Risks can occur at any layer of the information system:
 - At the physical hardware or device layer, e.g. when a flood renders servers stored in a basement unavailable;
 - At the various software layers, e.g. when hackers exploit a vulnerability in software;
 - At the network layer, e.g. when a hacker intercepts data packets as they pass through the network from sender, via routers, to receiver; or,
 - At the user layer, e.g. through 'social engineering', such as convincing users to share their passwords through 'phishing' emails

Risks III

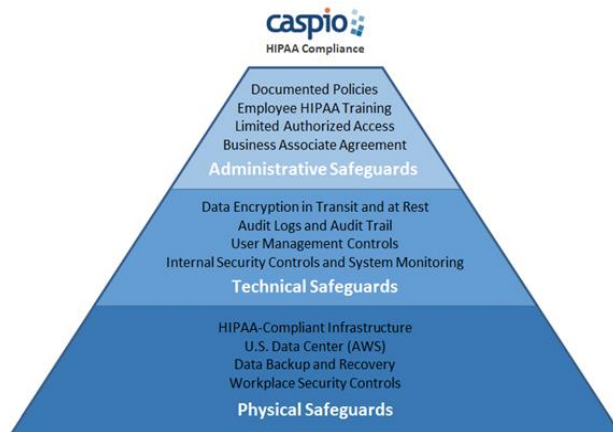
- Risk analysis and management to classify and respond to risks
- Probability a threat will exploit a vulnerability – high, medium, low
- Information security impact – loss of confidentiality, integrity and availability
- Other impacts – loss of life, productivity or profit, property and reputation
- Assessment of impact – address risks that have large impact on information security
- Types of responses: risk avoidance, risk mitigation, risk transfer, risk acceptance

Safeguards I

= safeguard reduces the harm posed by information security vulnerabilities or threats

1. Administrative – actions and rules implemented to protect information (need to know rule)
2. Technical – logical rules that state how systems will operate (least privilege rule)
3. Physical – actions to protect actual physical resources

Safeguards II



32

32

Safeguards III

- Safeguards can be put in place at all layers of the system:
 - At the physical hardware or device layer, e.g. by physically securing server rooms against flooding;
 - At the various software layers, e.g. by installing the latest patches;
 - At the network layer, e.g. by using virtual private networks ('VPN'); and,
 - At the user layer, by ensuring that all personnel receive appropriate training to recognise phishing emails and other forms of social engineering.

Exercise

- Fill in the missing terms:



If a company has an antivirus software but does not keep the virus signatures up-to-date, this is a The company is vulnerable to virus attacks.

The is that a virus will show up in the environment and disrupt productivity.

The likelihood of a virus showing up in the environment and causing damage is the

If a virus infiltrates the company's environment, then vulnerability has been exploited and the company is exposed to loss.

The in this situation are to update the signatures and install the antivirus software on all computers.

Information Security Management

- To effectively assess the security needs of an organization and to evaluate and choose various security products and policies
- Categorize information
- Identify legal obligations
- Assess vulnerabilities, threats and risks
- Safeguards
- There are a number of challenges
- Development of standards

ISO/IEC 27001

27001:2022 *Information Security Management Systems*

- The world's best-known standard for **information security management systems (ISMS)**
- It defines *requirements* an ISMS must meet
- The standard provides companies of any size and from all sectors of activity with guidance for establishing, implementing, maintaining and continually improving an information security management system
- Conformity with ISO/IEC 27001 means that an organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles

ISO/IEC 27002

27002:2022 Information security, cybersecurity and privacy protection — Information security controls

- This document provides a reference set of generic information security controls including implementation guidance
- This document is designed to be used by organizations:
 - within the context of an information security management system (ISMS) based on ISO/IEC27001;
 - for implementing information security controls based on internationally recognized best practices;
 - for developing organization-specific information security management guidelines
 - for identifying the objective for each control, how it works, and what companies can do to implement it successfully

ISO/IEC 27001

- *Specification* for an ISMS
- Way to measure, monitor and control security management from a top-down perspective
- Part 2 defines a six-step 'process', essentially:
 - Define a security policy
 - Define the scope of the ISMS
 - Undertake a risk assessment
 - Manage the risk
 - Select control objectives and controls to be implemented
 - Prepare a statement of applicability

Summary

- Information security is the study and practice of protecting information = valuable asset
- The main objectives of information security are to protect the confidentiality, integrity, and availability (CIA) of information
- Key information security concepts include vulnerabilities, threats, risks, and safeguards
- Legal duties and incentives to implement information security
- The importance of standards

Reading

'Cybercrime : protecting your business, your family and yourself, Todd Wade, BCS, 2022

Chapter 1 – Introduction

Available as an e-book on QMPlus



40