Week 3 Revision notes

IFB240 Week 3 - Managing Security

Overview

This week's lecture focused on **Information Security Risk Management** and the standards that guide effective security management practices. Key elements include the **risk management process**, detailed **risk assessments**, and how international standards like **AS/NZS 27001** and **AS/NZS 27002** help organisations systematically protect their information assets.

1. Why Manage Cyber/Info Security?

Regular Activities that Put Information Assets at Risk

- Many daily actions expose data and systems to threats, such as:
  - Using **email** with images, links, or attachments.
  - **Cloud storage** for data.
  - Using **mobile devices** (laptops, phones) and **portable storage** like USBs.
  - **Banking, shopping, gaming**, and **social networking** online.

Importance of Security Management

- Regular use of technology means that **information security risks are prevalent**. Protecting against these risks ensures that information remains **confidential, intact, and available** when needed.

Managing Information Security Involves Key Questions:

1. **What needs protection?** Identify your **information assets** and their location.
2. **Why protect these assets?** Consider **potential threats** and **vulnerabilities** that could lead to damage.
3. **What could go wrong?** Evaluate the **consequences** and **impact** if an asset is compromised.
4. **How can assets be protected?** Consider the **resources needed**, their costs, and how **urgently** protection is required.
5. **What happens if assets aren't protected?** Understand the **potential costs** of unaddressed vulnerabilities.
6. **Limited Resources**: We can't protect all assets from all threats—security is about **making tradeoffs** and **managing risk** effectively.

2. Understanding Risk in Information Security

Defining Risk

- **Risk** refers to the **effect of uncertainty** on objectives. It's usually assessed in terms of **likelihood** (chance of an event happening) and **consequences** (impact of that event).
- The **AS/NZS 27005:2012** standard defines risk in cybersecurity as involving **threats** exploiting **vulnerabilities** to cause harm to an asset.

Elements of Risk

1. **Likelihood**: Probability of an event occurring.
2. **Consequences**: Impact of the event on the organization's objectives.

Real-World Context

- **$1,000 financial loss** from a student’s bank account may have a much higher perceived impact compared to a bank losing the same amount. The **perception of impact** varies with the stakeholder's perspective.

Examples of Negative Events

- **Power loss** to systems or buildings.
- **Communication failures** in specific locations.
- **Data loss** or theft of **intellectual property**.
- **Public disclosure** of confidential information.

3. The Risk Management Process (AS/NZS 27005:2012)

Overview of the Process

1. **Establish the Context**:
    - **External Context**: Relationship between the organization and its environment.
    - **Internal Context**: Organization’s goals, objectives, and capabilities.
    - **Risk Management Context**: Define the **criteria for evaluating risks**, considering asset value, impact on operations, and legal obligations.
2. **Risk Assessment**:
    - **Risk Identification**: Identify assets, plausible threats, existing controls, and vulnerabilities.
    - **Risk Analysis**: Determine the **magnitude** of identified risks using either **qualitative** or **quantitative** methods.
        - **Qualitative Analysis**: Descriptive scales (e.g., minor, major, catastrophic).

        - **Quantitative Analysis**: Numerical scales (e.g. value, probability).
    - **Risk Evaluation**: Compare identified risks against risk criteria to prioritise actions.
3. **Risk Treatment**:
    - **Options** include:
        - **Risk Avoidance**: Stop activities that introduce the risk.
        - **Risk Modification**: Apply controls to reduce **likelihood** or **consequences**.
        - **Risk Sharing**: Transfer the risk to another party (e.g., insurance).
        - **Risk Retention**: Decide not to act, accepting the risk.
4. **Monitoring and Review**:
    - Ongoing reviews are crucial to assess:
        - Changes in the **likelihood or consequence** of identified risks.
        - Effectiveness of **risk treatment plans**.
    - Example: **Netgear discontinued support** for older routers, making them vulnerable to attacks—highlighting the importance of reviewing security posture as circumstances evolve.

4. Information Security Standards Overview

AS/NZS 27001:2023 and AS/NZS 27002:2022

- **AS/NZS 27001**: Focuses on establishing, implementing, and continually improving an **Information Security Management System (ISMS)**.
    - **Certification** is possible under this standard, demonstrating a company's commitment to information security.
- **AS/NZS 27002**: Provides **guidance on security controls** for information management. It serves as a practical tool for implementing the security measures outlined by **AS/NZS 27001**.

Structure and Key Clauses

- **Clause 4**: Establishing the **context of the organization** for implementing an ISMS.
- **Clause 6**: Planning, which includes **risk assessment** and **risk treatment** processes.
- **Clause 8**: Operational planning, where security controls are implemented.
- **Clause 10**: Continuous **improvement** of the ISMS, adapting to new risks and challenges.

Importance of Standards

- Applying these standards helps organizations ensure **consistent and comprehensive protection** of information assets.
- **Certification** under **AS/NZS 27001** offers **assurance** that proper security management practices are in place and helps to instill confidence in customers and stakeholders.

5. NIST Cybersecurity Framework (CSF)

- **NIST CSF** is another widely used framework that provides a structured approach to managing and reducing cybersecurity risks.
  - **Five Functions**: **Identify, Protect, Detect, Respond, Recover**.
  - Particularly useful for critical infrastructure and is designed for **risk-based decision-making**.
  - **Version 2.0** (published in February 2024) emphasizes **governance and supply chains**, making it more adaptable to emerging threats.

Key Differences from ISO Standards

- Unlike the ISO27K series, which is more descriptive and process-based, **NIST CSF** is structured into functional domains, making it more **action-oriented**.
- Both frameworks are risk-based, but NIST's emphasis is on **actionable steps** for each function, tailored to an organization's unique environment.

6. Risk Analysis: Qualitative vs Quantitative

Types of Analysis

- **Qualitative Analysis**:
  - Uses descriptive categories (e.g., **minor, moderate, catastrophic**).
  - Suitable when data is scarce, such as assessing the potential impact of new threats.
- **Quantitative Analysis**:
  - Uses numerical scales (e.g. values, **probability from 0 to 1**).
  - Suitable when accurate data on risk frequency and impact is available.

Example:

- **Risk Assessment for Found USB Drives**:
  - **Quantitative Analysis**: Use metrics like the percentage of users who plugged in a found USB (e.g., "50% of users plugged in found USB drives").
  - **Qualitative Analysis**: Describing the potential consequences as **high** or **moderate** based on historical incidents.

7. Real-World Examples and Emerging Risks

Case Study: Netgear Routers

- **Vulnerability**: Netgear discontinued support for older routers, leaving them vulnerable to exploitation.
- **Impact**: Customers using unsupported devices face increased risk, especially with the growing trend of **remote work**, which places more reliance on secure home networks.

Case Study: Equifax Data Breach (2017)

- **Data Compromised**: Personal identifiable information (PII) for over 145 million people.
- **Impact**: Significant reputational and financial consequences, leading to regulatory scrutiny.
- **Key Lesson**: The need for **effective incident response** and **continual improvement** in risk management practices to prevent recurring issues.

8. Summary and Key Takeaways

- **Information Security Risk Management** is about understanding what needs protection, why, and how to protect it within the available resources.
- **Risk Assessments** are central to effective management, allowing for prioritizing actions to mitigate risks.
- **Security Standards** (e.g., AS/NZS 27001 and AS/NZS 27002) provide a framework for organizations to systematically manage and protect their information assets.
- **Monitoring and Review** is crucial for adapting to new threats and ensuring that controls remain effective over time.
- **Real-world examples** like Netgear and Equifax show the practical importance of **continuous monitoring**, **risk analysis**, and **adaptive risk management** to secure information in an evolving landscape.