WOA7017: Security Risk Analysis and Evaluation - Expanded Study Notes

Instructor: Prof. Ts. Dr. Omar Zakaria *(Contact: 012-9180186, manafzack@gmail.com)*

Week 1: Introduction and Foundational Concepts

- **Focus:** This week introduces the 'why' and 'what' of security risk assessment (SRA), the role of the security manager in this process, and how SRA differs from related activities like audits or penetration tests.

1. The Role of the Information Security Manager: * The Information Security Manager (ISM) is central to protecting an organization's information assets. Their responsibilities directly tie into the need for risk analysis: * **Preventing loss, fraud, and data breaches:** Understanding risks helps prioritize defenses against financial loss, reputational damage, and theft of sensitive data. * **Demonstrating regulation compliance:** Many regulations (like GDPR, HIPAA, local laws) require risk assessments. The ISM uses SRA results to prove due diligence and meet legal/regulatory obligations, avoiding fines and sanctions. * **Managing security policies:** Policies should be informed by risk. The ISM ensures policies are relevant, implemented, and address identified risks. * **Ensuring business continuity:** SRA identifies threats to critical business functions. The ISM uses this to develop plans (BCP/DRP) ensuring the business can operate during and after disruptions. * **Planning incident and disaster response:** Knowing potential risks allows for tailored incident response plans, making reactions faster and more effective. * **Prioritising security initiatives:** Resources (time, money, people) are always limited. SRA helps the ISM justify and direct spending towards the most significant threats, maximizing the return on security investment.

2. Approaches to Identify & Prioritise Security Initiatives: * Organizations decide where to spend security resources based on different drivers: * **Audit as a Driver:** Findings from internal or external audits highlight weaknesses or non-compliance. Initiatives focus on fixing these specific audit points. *Pro: Addresses known issues. Con: Can be reactive, might miss non-audited risks.* * **Technology as a Driver:** Focus is on acquiring the latest security technology (e.g., next-gen firewall, EDR). *Pro: Can improve capabilities. Con: May not address the actual biggest risks, could be expensive, might ignore process/people issues.* * **Compliance as a Driver:** Initiatives aim solely at meeting the requirements of a specific standard or regulation (e.g., ISO 27001, PCI DSS). *Pro: Achieves compliance. Con: Meeting the minimum requirement might not be secure enough; "checkbox security".* * **Security Risk as a Driver: (Often considered the most effective approach)** Initiatives are prioritized based on the results of a formal SRA, targeting the highest risks to the organization's mission and assets. *Pro: Focuses resources efficiently, addresses actual threats, provides justification for spending. Con: Requires a quality SRA process.*

3. Ensuring a Quality Information Security Risk Assessment: * A high-quality SRA is crucial for effective security management. * **Why Quality Matters:** * It provides credible evidence that security efforts address the *most important* risks. * It forms a rational basis for security decisions, strategy, and budget allocation. * **Consequences of a Weak SRA:** * **False conclusions:** Believing you are secure when you are not, or focusing on minor issues. * **Biased results:** Skewed findings due to poor methodology, lack of objectivity, or influence from specific departments. * **Significant planning errors:** Investing in the wrong controls, inadequate protection for critical assets. * **Increased security risks:** Ultimately, a poor assessment can lead to a weaker security posture than doing nothing, as it creates a false sense of security.

4. Security Risk Assessment (SRA): * **Core Role:** To systematically identify, analyze, and evaluate risks to information assets. * **Analysis of Control Effectiveness:** SRA doesn't just assume controls work; it involves *testing and reviewing* them (e.g., checking firewall rules, testing backups, vulnerability scans, observing physical access). * **Informing Risk Mitigation:** Based on the analysis, decisions are made on how to treat the risk: * **Accept:** If the risk is low or the cost of mitigation is too high. * **Reduce:** Implement or improve controls to lower the likelihood or impact. (This is the most common). * *(Transfer/Share is another option, often covered later - e.g., insurance, outsourcing)*. * **Impacting Operational Security:** SRA findings highlight where operational staff (IT, users) need better training, awareness, or procedures to maintain security effectively. * **Definition:** While definitions vary (NIST, ISO, SOX), the essence is: * *"A probability determination of asset losses based on asset valuation, threat analysis, and an objective review of current security controls effectiveness."* * **Key Components:** Assets (what we protect), Value (how important?), Threats (what can cause harm?), Vulnerabilities (weaknesses threats exploit), Controls (existing protections), Likelihood (probability of occurrence), Impact (consequences of loss). * **Need for SRA:** * **Checks and Balances:** Provides an objective review of how well assets are *actually* protected, beyond just assuming policies are followed. * **Periodic Review:** The threat landscape, business objectives, and technology constantly change. SRA must be repeated periodically (e.g., annually or after major changes) to remain relevant. * **Risk-Based Spending:** Justifies security expenditures by linking them directly to the reduction of specific, identified risks. Helps answer "Are we spending money on the right things?". * **Secondary Benefits (Often Overlooked but Valuable):** * **Knowledge Transfer:** Assessment team (internal or external) shares expertise with internal staff during the process. * **Increased Communication:** SRA often requires input from different departments (IT, HR, Legal, Business Units), fostering dialogue about security responsibilities. * **Increased Security Awareness:** The process itself (interviews, observations) raises awareness among employees about security threats and practices. * **Benchmarking:** Results provide a baseline to measure the security program's improvement over time. * **Skill Development:** Develops internal capabilities in risk assessment and security analysis. * **Holistic View:** Highlights how security controls in different areas (physical, technical, administrative) interact and depend on each other. * **Documented Risk Profile:** Creates a formal record of the organization's key risks.

5. Related Activities (Distinctions are Important): * These activities are related to security assessment but have different specific goals: * **Gap Assessment:** * *Focus:* Comparing current controls against a *specific standard* (e.g., ISO 27001 Annex A, NIST CSF). * *Outcome:* A list of controls that are missing or deficient to meet that standard. *Purpose is compliance readiness.* * **Compliance Audit:** * *Focus:* Verifying if *required* controls (by law, regulation, or standard) are implemented and operating as intended. * *Outcome:* An attestation (formal statement) of compliance or non-compliance. *Purpose is formal verification.* * **Security Audit:** * *Focus:* Verifying if *specified* security controls (often based on internal policy or industry best practices) are in place and effective. Broader than compliance audit. * *Outcome:* Attestation of adherence to chosen standards/policies. *Purpose is verification against chosen benchmarks.* * **Penetration Testing (Pen Test):** * *Focus:* Simulating an attack to actively exploit vulnerabilities and test the *effectiveness* of defenses. Methodical and planned. * *Outcome:* Report detailing vulnerabilities found, how they were exploited, and the potential impact. *Purpose is testing control adequacy under attack.* * **Vulnerability Scanning:** * *Focus:* Using automated tools to scan systems for *known, common* vulnerabilities and configuration weaknesses (the "low-hanging fruit"). Often a part of a pen test. * *Outcome:* List of potential vulnerabilities detected by the scanner. *Purpose is finding obvious weaknesses quickly.* * **Ad Hoc Testing:** * *Focus:* Less structured testing, often relying on expert intuition and experience to find *less obvious* or novel vulnerabilities missed by automated scans or standard methodologies. * *Outcome:* Discovery of potentially complex or unique flaws. *Purpose is deeper, expert-driven vulnerability discovery.* * **Social Engineering:** * *Focus:* Testing the 'human element' – assessing awareness, training, and policy adherence by attempting to trick people into revealing information or granting access (e.g., phishing, pretexting). * *Outcome:* Assessment of susceptibility to manipulation. *Purpose is testing human defenses*.