Andree Salvo

Southern New Hampshire University

7-2 Project Three Submission: Crafting and Evaluating Risk-Based Recommendations

Instructor: Johnathan Hammitt

Making risk-informed decisions is a crucial aspect of cybersecurity, as it enables organizations to act before problems escalate into breaches. The 2015 Office of Personnel Management (OPM) breach is a strong example of what happens when risks aren't being properly managed. According to Secpod "The attackers were able to steal personal data from over 21 million federal employees, contractors, and families because of poor encryption, weak access controls, and outdated systems." (Secpod, 2024) In this paper, I'll discuss how using risk tools, industry standards, and systems thinking can lead to smarter, more ethical, and effective decision-making in cybersecurity.

Utilizing tools such as risk registers and business impact analyses (BIAs) enables organizations to identify and help prioritize potential threats before they escalate into significant issues. These tools allow decision-makers to track vulnerabilities, estimate the impact of disruptions, and prioritize fixes. Tools, such as **Threat modeling**, are useful for predicting how attackers might target systems/networks and identifying potential vulnerabilities. For instance, when utilizing these tools to assess outdated systems and encryption deficiencies, OPM could have identified the risk's severity earlier on and prioritized system upgrades to prevent the 2015 breach.

Utilizing resources such as the NIST Cybersecurity Framework (CSF) and CIS Controls enables organizations to make consistent, evidence-based decisions. Reviewing these resources outlines best practices for identifying assets, data, and monitoring threats. According to NIST (2018), the framework “allows organizations of any size, risk level, or cybersecurity maturity to use risk management principles and best practices to strengthen the security, defense, and resilience of critical infrastructure.” (NIST, 2018) If OPM had applied the NIST CSF and CIS Controls before 2015, it could have strengthened its asset management, improved encryption, and enhanced access controls, making it much harder for attackers to move unnoticed through its network without detection.

Bias can affect how cybersecurity professionals judge the importance of risks. For instance, optimism bias may cause teams to overestimate or assume that an attack is unlikely or that current controls are “ too good enough.” At OPM, leadership ignored repeated warnings about weak security, believing their system was safe enough. To minimize bias, organizations should use data-driven assessments, seek multiple viewpoints, and apply objective risk scoring. Regular reviews and third-party audits will also help keep decisions well-grounded in evidence rather than personal assumptions or overconfidence.

Systems thinking encourages organizations to consider the interplay between people, processes, and technology when making security-related decisions. Any modification impacts multiple parts of the system. For instance, if OPM had updated their outdated systems sooner, it would have required better employee training, revised procedures, and new security policies. Overlooking these interactions can result in implementation gaps. By employing systems thinking, all components are aligned to function cohesively, reducing human error and supporting both productivity and security for the organization to follow through**.**

A strong risk-based decision should lead to improvement over time, verified through evidence and performance metrics. Organizations can progress by tracking incidents, audit findings, and vulnerability scanning outcomes. For example, after the 2015 OPM breach, enhanced security post-breach could be reflected in fewer intrusion attempts, quicker detection, and stronger compliance results. Ongoing monitoring and post-incident evaluations can ensure that implemented controls effectively reduce the risks and safeguard sensitive data.

Resources

Sree, C. (2024, November 29). *Story of a cyberattack – OPM breach*. SecPod. https://www.secpod.com/blog/story-of-a-cyberattack-opm-breach/

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018