Assignment 2.1: Risk Types

Joshua A Wortz

University of San Diego

Course Number: CSOL-500

Dr. Michelle Moore

01/20/2024

Assignment 2.1: Risk Types

Organizations face many types of cyber risks. Schreider categorized risks into either compliance, financial, operational, or strategic (2019, p. 164). A risk is the likelihood of a threat actor exploiting a vulnerability. I chose operational risks in cybersecurity because these are an ever-present challenge for organizations, with data theft ranking among the most critical threats. Data theft can result in significant financial losses, reputational damage, and erosion of customer trust. Effective management of these risks requires a clear understanding of organizational risk tolerance—a concept determining the importance of addressing specific threats (Schreider, 2019, p. 166). A low-risk tolerance reflects the importance of protecting sensitive data and demanding stricter controls. By categorizing risks and applying the four approaches—Mitigation, Transfer, Accept, and Avoid—organizations can effectively align their strategies with risk tolerance levels to protect critical assets (Brown, 2023, p. 45).

Mitigation involves reducing the likelihood or impact of data theft by implementing proactive measures. For organizations with a low-risk tolerance, the focus is on deploying advanced security controls. These controls include encryption for sensitive data, real-time threat monitoring, and regular employee training to prevent insider threats and phishing attacks. For instance, encrypting customer data ensures that even if unauthorized access occurs, the stolen data remains unusable without decryption keys. Regular penetration testing and vulnerability scans enhance protection by identifying and addressing security gaps.

Strong but less intensive measures are sufficient in scenarios where the risk tolerance is moderate. Multi-factor authentication (MFA), endpoint protection, and periodic security audits

can effectively manage risks for systems of moderate importance. Organizations with high-risk tolerance might apply basic controls such as software updates and limited access restrictions, focusing on lower-priority systems that do not handle sensitive information. Tailoring mitigation strategies to the organization's risk tolerance can balance security with operational efficiency.

Risk transfer shifts the responsibility of managing specific risks to a third party. This approach is particularly relevant for organizations that lack the internal resources to manage data theft risks independently. For organizations with a low-risk tolerance, this might involve contracting with highly specialized cybersecurity firms to monitor networks and detect potential breaches. These third parties must demonstrate robust compliance with security standards to ensure the integrity of sensitive data.

Organizations with moderate risk tolerance might transfer risks associated with medium-priority tasks, such as regular vulnerability assessments or system monitoring, to reputable vendors. In contrast, those with high-risk tolerance may use standard service-level agreements (SLAs) to outsource non-critical functions without the same level of scrutiny. For example, a low-tolerance organization might engage a managed detection and response (MDR) service to provide 24/7 threat monitoring and incident response, ensuring continuous protection against data theft.

Risk acceptance involves tolerating certain risks when mitigation or transfer is impractical or unnecessary. For organizations with a low-risk tolerance, accepting risks is rare and typically reserved for situations where residual risks are minimal and heavily documented.

For example, an organization might temporarily accept minor risks during a system migration while ensuring robust monitoring and contingency plans are in place.

With moderate risk tolerance, organizations may accept risks associated with legacy systems that impact operations but do not handle highly sensitive data. The team should document in a risk register with a clear plan for eventual resolution. In cases of high-risk tolerance, acceptance is more common and may involve minimal monitoring of risks deemed low priority. For instance, a company might allow temporary vulnerabilities in non-critical systems, provided there is no immediate threat to sensitive data or operations.

Risk avoidance focuses on eliminating activities or conditions that create exposure to data theft. For organizations with a low-risk tolerance, avoidance is a primary strategy. These organizations proactively eliminate high-risk practices, such as using unencrypted communication channels or storing sensitive data on portable devices. Data minimization, where only essential information is collected, is another effective avoidance technique as it reduces exposure to potential threats.

Organizations with moderate risk tolerance might avoid practices with moderate exposure, such as outdated software or weak authentication mechanisms. In contrast, those with high-risk tolerance may see avoidance as unnecessary for low-priority risks, as other strategies like mitigation or acceptance may suffice. For example, a low-tolerance organization might discontinue sharing accounts for critical systems to ensure accountability and reduce unauthorized access risks.

Managing operational risks such as data theft requires organizations to align their strategies with risk tolerance levels. A low-risk tolerance necessitates comprehensive measures to mitigate, transfer, or avoid risks, protecting critical assets and maintaining customer trust. Moderate and high-risk tolerances allow for more flexible strategies, balancing security with operational efficiency. By categorizing risks and applying tailored management approaches, organizations can build resilient systems that effectively address the challenges of data theft while supporting their overall objectives.

References

Brown, J. (2023). *Executive's Cybersecurity Program Handbook: A Comprehensive Guide to Building and Operationalizing a Complete Cybersecurity Program*. Packt Publishing, Limited.

Schreider, T. (2019). *Building an Effective Cybersecurity Program, 2nd Edition* (2nd ed.). Rothstein Publishing.