Evaluating the Risk Management Framework and Assessing Internal Risks

IT-FPX4076

Leo Newton

11/16/2024

Introduction

The National Institute of Standards and Technology (NIST) publications 800-37 Revision 2 and 800-30 Revision 1 provide comprehensive guidance for assessing and managing risk within organizations. NIST SP 800-37 outlines the Risk Management Framework (RMF), a structured and flexible process for managing security and privacy risk, while SP 800-30 specifically addresses risk assessment methodologies (NIST, 2018). Together, these publications offer a powerful framework for identifying, analyzing, and mitigating internal risks.

The Role of the RMF and SP 800-30 in Internal Risk Assessment

The RMF (NIST SP 800-37) provides a systematic approach to managing risk, encompassing the entire system development life cycle (SDLC) (NIST, 2018). It comprises seven steps: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor. Each step involves specific tasks to be performed by designated individuals or teams within the organization. SP 800-30 enhances the RMF by delving into the specifics of risk assessment, providing methodologies and templates to identify threats, vulnerabilities, likelihoods, and impacts.

Specifically relating to internal risk, the RMF and SP 800-30 contribute in several ways:

* Identifying Internal Threat Sources: SP 800-30 provides a taxonomy of threat sources, including insiders (e.g., malicious insiders, accidental insiders). This helps organizations recognize that employees can pose a risk, whether intentionally or unintentionally. The RMF tasks related to personnel security and access control further address this internal threat vector.
* Assessing Vulnerabilities Related to Employee Actions: Both publications emphasize the importance of identifying vulnerabilities that can be exploited by internal actors. This includes vulnerabilities in policies, procedures, and technologies, such as weak passwords, inadequate access controls, or lack of data loss prevention measures.
* Analyzing the Impact of Internal Events: The RMF and SP 800-30 guide organizations in analyzing the potential impact of internal events, such as data breaches caused by employee negligence or malicious acts (NIST, 2012). This involves assessing the financial, operational, and reputational consequences of such events.
* Developing Mitigation Strategies: The RMF emphasizes the development and implementation of security and privacy controls to mitigate identified risks. This includes technical controls (e.g., encryption, access control lists), operational controls (e.g., background checks, security awareness training), and management controls (e.g., policies, risk assessments). SP 800-30 provides additional context for these efforts (NIST, 2012).
* Monitoring and Responding to Internal Risks: The Monitor step of the RMF highlights the need for continuous monitoring to detect changes that may affect the security and privacy posture of the organization. This includes monitoring employee behavior, system logs, and security alerts to identify potential internal threats.

Internal Risks from Social Media and Digital Communication Channels

Employee use of social media and digital communication channels presents several internal risks:

* Data Leaks: Employees may inadvertently disclose confidential information or intellectual property through social media posts or other digital communications.
* Phishing and Social Engineering: Employees may fall victim to phishing attacks or social engineering scams launched through social media or messaging platforms, providing attackers with access to organizational systems or data.
* Reputational Damage: Negative social media posts or online comments by employees can damage the organization’s reputation.
* Malware Propagation: Employees may click on malicious links or download infected files from social media or messaging platforms, introducing malware into the organization’s network.

Internal Risks from Non-Company Devices

Employee use of personal smartphones and tablets (BYOD) introduces further internal risks:

* Data Loss or Theft: Non-company devices are more susceptible to loss or theft, potentially exposing sensitive organizational data stored on those devices.
* Malware Infections: Non-company devices may lack the same level of security protection as company-managed devices, increasing the risk of malware infections that can spread to the organization's network.
* Data Leakage through Unsecured Apps: Employees may use unsecured apps on their personal devices to access or store organizational data, creating a potential data leakage channel (Scarveles, 2014).
* Lack of Visibility and Control: IT departments have limited visibility and control over non-company devices, making it difficult to enforce security policies and monitor data access.

Conclusion

The NIST RMF and SP 800-30 provide a robust framework for assessing and managing internal risks (NIST, 2012). By systematically identifying threat sources, vulnerabilities, likelihoods, and impacts, organizations can develop and implement effective mitigation strategies to reduce the risk posed by employee actions and the use of technology. Addressing the specific risks associated with social media, digital communications, and non-company devices requires a combination of technical controls, user education, and clear policies to mitigate the potential for data breaches, malware infections, and reputational damage.

References

NIST. (2018). *NIST Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

NIST. (2012). *NIST Special Publication 800-30 Revision 1, Guide for Conducting Risk Assessment*s.

Scarveles, S. (2014) *NIST SP 800-121, Guide to Bluetooth Security*. National Institute of Standards and Technology (NIST).