Information Security Management Models

Ryan Coon

CYB-535

Dr. Edward Marchewka

January 22, 2025

**Mission statement**

At RC Cybersecurity, our mission is to protect the digital landscape of businesses and individuals by providing comprehensive and innovative cybersecurity solutions. We are committed to proactive defense, utilizing state-of-the-art technology to anticipate, detect, and neutralize threats before they can cause harm. Our approach emphasizes empowerment through knowledge, as we believe that educating our clients is crucial in fostering a culture of cybersecurity awareness. By offering tailored solutions that align with each client’s unique needs, we ensure that they are equipped to tackle their specific challenges. Integrity and trust are at the core of our operations, guiding our relationships with clients through transparency and ethical practices.

**Web applications**

RC Cybersecurity utilizes a variety of web applications to enhance its cybersecurity measures and streamline operations. Among those are vulnerability management tools and secure collaboration and communication applications.

**Servers**

RC Cybersecurity implores multiple servers to keep each company operation separate. This includes separate mail servers, application servers and database servers. These servers work together to create a comprehensive cybersecurity framework, enabling RC Cybersecurity to protect its assets effectively and respond to potential threats.

**Departments**

When dealing with the various aspects of cybersecurity, our departments include Information security, IT, Cybersecurity operations, Compliance and Risk management, and Research and Development.

**Routers and switches**

Routers and switches are essential elements of our network infrastructure, as they manage data traffic between devices and facilitate efficient communication throughout our customers' networks.

**Remote access**

Solutions are provided to remotely access their workstations. Authorized users can then work remotely while paired with a VPN to connect with a secure connection.

**Wireless communication**

A strong Wi-Fi solution is implemented to accommodate a high density of users and guarantee reliable connectivity, while within company grounds.

**Firewalls**

Firewalls are utilized to prevent unauthorized access and potential cyber threats, safeguarding the customer's network. They filter incoming and outgoing traffic according to security rules, which helps protect our IT infrastructure from malicious activities.

**Demilitarized zone (DMZ)**

A network segment or DMZ is utilized to separate the company’s internal network from the external network. This will separate the customers outward facing services such as websites from the data sensitive internal network.

The NIST Cybersecurity Framework is voluntary guidance, based on existing standards, guidelines, and practices to help organizations better manage and reduce cybersecurity risk(NSIT, n.d.). RC Cybersecurity, a proactive cybersecurity firm, will strategically implement the NIST Cybersecurity Framework (CSF) by focusing on its critical security activities. First, the company will identify its assets and conduct comprehensive risk assessments to establish a clear understanding of vulnerabilities. In the protect phase, rigorous access control measures and employee training programs will be introduced to safeguard sensitive information. Continuous monitoring and vulnerability scanning will be employed to enhance the detect phase, ensuring real-time identification of potential threats. For the respond phase, RC Cybersecurity will develop a robust incident response plan and establish clear communication protocols to manage incidents effectively. Finally, in the recover phase, the organization will implement recovery planning and regular data backups to ensure business continuity.

Ransomware attacks continue to be a pervasive threat, with cybercriminals targeting organizations across various sectors, often resulting in substantial financial losses and operational disruptions. Additionally, phishing and social engineering tactics have become increasingly sophisticated, as attackers craft convincing messages to deceive individuals into divulging sensitive information or credentials. Insider threats also remain a critical concern, as employees may inadvertently or maliciously compromise sensitive data. Furthermore, vulnerabilities within the supply chain have emerged as a significant risk, with attackers exploiting weaknesses in third-party vendors to gain unauthorized access.

To develop system-specific plans for the protection of intellectual property (IP), RC Cybersecurity would undertake a systematic approach, focusing on key areas such as access control and data protection strategies. We would Implement role-based access controls (RBAC) to ensure that only authorized personnel can access sensitive IP information and utilize strong authentication methods, such as multi-factor authentication (MFA), to enhance security. To protect data, we would encryption for both stored and transmitted IP data to prevent unauthorized access and implement DLP solutions to monitor and control data transfers, reducing the risk of IP leaks.

At RC Cybersecurity, implementing robust access control mechanisms is essential for ensuring that information is protected against unauthorized users. The company would adopt a multi-layered approach to access management, beginning with role-based access control (RBAC), where permissions are assigned based on user roles within the organization. This ensures that employees only have access to the information necessary for their job functions(FyndAcademy, 2024). Additionally, multi-factor authentication (MFA) would be mandated for all users, adding an extra layer of security by requiring multiple forms of verification before granting access. Regular access reviews would be conducted to ensure that user permission remain aligned with job responsibilities and to identify any potential orphaned accounts or outdated access rights.

Regarding the roles involved in the planning and management of the security plan, particularly through the lens of C-level functions that influence cybersecurity, the following personnel play a significant role.

**Board of Directors**

Responsible for ensuring that the organization has an effective cybersecurity strategy in place. They set the tone for security priorities and allocate necessary resources. They assess the overall risk posture of the organization and ensure that cybersecurity risks are integrated into the company's broader risk management framework.

**Senior Management**

Responsible for establishing the vision and strategic direction for cybersecurity initiatives, ensuring they align with business objectives. They are also responsible for allocating the necessary resources and budget to effectively implement and maintain the cybersecurity plan.

**Chief Information Security Officer (CISO)**

Spearhead the development and execution of the cybersecurity strategy, ensuring alignment with organizational objectives. They create and enforce cybersecurity policies, standards, and procedures, while also overseeing risk assessments and incident response plans.

**IT Management (CIO, IT Director, etc.)**

Oversee the organization’s IT infrastructure and ensure it is secure and resilient against cyber threats. They are responsible for selecting, implementing, and managing security technologies and solutions that protect information assets.

**Functional Area Management**

Ensure that cybersecurity policies are integrated into their departmental processes and workflows and that their teams are compliant with cybersecurity protocols and participate in training initiatives to foster a culture of security awareness.

**Information Security Personnel**

Oversee daily security operations, which include monitoring systems, responding to incidents, and performing vulnerability assessments. They analyze security incidents to enhance defenses and offer insights into emerging threats and security trends.

**End Users**

Play a vital role in cybersecurity, often serving as the first line of defense against cyber threats. It is essential for them to adhere to established security protocols and engage in training to comprehend the significance of cybersecurity measures and their responsibilities in safeguarding the organization.

References:

*FyndAcademy. (2024, November 25). Importance of Cyber Security (Types & Career Opportunity in 2025). Fynd.academy; FyndAcademy. https://www.fynd.academy/blog/importance-of-cyber-security*

*Getting Started with CSF 1.1. (2018). NIST. https://www.nist.gov/cyberframework/background*

*Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide. (n.d.). https://csrc.nist.gov/CSRC/media/Projects/cybersecurity-framework/documents/Framework\_Quick%20Start\_Guide.pdf*