The Significance of Roles in Cybersecurity (Module 7): Addressing Risks and Legal Issues

Tyler Postma, Sai Parwatha, Logan Lyons, Zane Zahid

Central Michigan University

Course# 22445811: BIS521

Professor Helser

February 18, 2024

**Security Managers**

Examining the risk and legal issues associated with the roles of Security Managers in cybersecurity is crucial in understanding their role's significance. Analyzing the challenges and potential legal implications faced by Security Managers in their day-to-day responsibilities highlights the importance of their day-to-day responsibilities. The dynamic nature of cybersecurity and the challenges faced by Security managers as they navigate complex cyber threats while adhering to risk and legal issues is vital for a corporation's systems.

The IT Security Manager focuses on developing and managing compliance programs and ensuring coherence throughout the system's life cycle. A strong emphasis is placed on continuous risk management, especially concerning new software development, aligning closely with the guidelines outlined by NIST.

Security Managers are tasked with ensuring strict adherence to legal requirements, especially those outlined by the NIST framework. This includes conducting regular risk assessments to identify potential cybersecurity risks and implementing risk management plans to mitigate the identified risks. (Wilson, 2006) They must regularly assess systems in accordance with NIST guidelines and incorporate incident response plans that align with NIST standards that entail periodic drills and simulations to ensure the effectiveness of security responses.

The responsibility for incident response management and conducting investigations into security breaches in the Security Manager role highlights the legal implications of potential security incidents. Legal implications can arise due to the sensitive nature of data and its potential impact on the organization. Compliance with data protection laws and regulations becomes crucial during the incident response process to avoid legal consequences.

Security managers deal with significant responsibilities while focusing on risk assessment, management, and legal compliance. Continuous efforts in compliance, routine risk evaluations, and proficient handling of legal considerations are vital in day-to-day operations. With increasing regulatory assessment pressures, security managers must stay informed about legal frameworks, ensuring both compliance and resilience against potential legal consequences.

**Security Analyst**

A security analyst is a broad, rapidly evolving role that entails safeguarding an organization’s data. The role serves as a connection point between business and technical teams. Duties often include vulnerabilities and threat hunting, systems, and network maintenance, designing and implementing data governance, and ensuring compliance with relevant laws and best practices.

The common responsibility of a security analyst is to safeguard and prevent cyber-attacks. The specific work criteria depend on the organization. It is much easier and inexpensive to protect the data from security threats rather than trying to recover the data from threats.

A security analyst faces important risks and responsibilities when responding to and managing security incidents in an organization.

Missing a critical indicator of compromise can allow an attack to spread farther across the network. There is a risk that an incident response is not initiated fast enough. Improper containment or system shutdowns during an incident response can cause significant business disruption if executed haphazardly. There are risks to productivity if incidents are not handled precisely.

Carefully follow the procedures and checklists outlined in the organization's incident response plan when reacting to a security event. Analysts have a responsibility to adhere to response protocols. Prioritize incidents using a standard rating system when the security team faces multiple simultaneous threats, so the most dangerous situations get addressed first. Analysts must judge event severity responsibly.

In addition, security analysts are expected to have expertise in cyber security, firewalls, network security, information assurance, Linux, UNIX, security information and event management (SIEM), application security, security engineering, and security architecture. They must also keep up with the latest trends in cyber security.

The most successful analysts are detail-oriented and have an analytical mindset. Security analysts work with scenarios – and this could mean pouring over thousands and thousands of pages of data to look for anomalies. Interpersonal skills are also crucial; analysts need to train company staff on better security protocols and regularly communicate with executive leadership.

**Chief Security Officer (CSO)**

A CSO represents an organization's first line of defense when it comes to cybersecurity. In the ever-evolving landscape of cybersecurity, organizations are increasingly reliant on skilled professionals to fortify their digital perimeters. Special focus on the significance of each role in mitigating risks and addressing legal concerns. Among these roles is the Chief Security Officer (CSO), unraveling the unique responsibilities and contributions that define this crucial position. Understanding these roles is paramount in establishing a robust defense against cyber threats and ensuring compliance with legal standards.

The role involves not only formulating but also implementing comprehensive security measures, leveraging cutting-edge technologies such as intrusion detection systems and firewalls. As a leader in the cybersecurity domain, CSO’s decisions significantly impact the overall business function.

A key component of the CSO's duties is legal compliance, which entails closely examining the laws and rules that are relevant to cybersecurity. CSO negotiates the complex web of regulatory frameworks to make sure the company follows the rules.

The complex legal framework that oversees information security regulations is always evolving to address new threats to the sector. CSOs are responsible for ensuring compliance with regulations such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), depending on the organization's nature.

Noncompliance may result in severe legal consequences, such as fines and damage to one's reputation. Real-world case studies can emphasize the consequences of legal non-compliance for firms and the need for CSOs to stay current with evolving legal requirements.

In a well-reported instance, when patient records were exposed because of insufficient cybersecurity safeguards, a healthcare organization was subject to harsh legal repercussions. In this case, the CSO played a key role in coordinating with regulatory agencies to minimize the legal ramifications, guaranteeing adherence to health data privacy regulations, and carrying out an exhaustive internal investigation. This illustration highlights how crucial the CSO is to handle legal complexity and preserve the organization's integrity in the face of possible legal penalties.

Furthermore, a large international company was hit with heavy fines after a data breach revealed private client data. This issue could have been avoided if the CSO had complied with legal requirements and laws. This shows how serious non-compliance can be and how crucial a proactive CSO is to maintain the organization's legal status.   
  
 Moreover, the influence of the CSO reaches into the strategic domain of corporate operations. In a real-world instance, the CIO and CSO of a top technology business worked together to design and execute a safe yet intuitive authentication system. The implementation of this measure not only improved the cybersecurity posture of the firm but also enabled a smooth user experience, underscoring the importance of the CSO in promoting a comprehensive approach to cybersecurity.

As many real-world instances demonstrate, a company's total security posture greatly depends on the CSO's ability to manage legal and risk issues. Their concrete impact on preventing data breaches, ensuring legal compliance, and overcoming human problems highlights their significance as strategic leaders in guarding against cyber threats.

**Chief Information Security Officer**

Despite not usually being an executive position, the Chief Information Security Officer (CISO) provides a critical role in an organization. This role serves as a facilitator between the technical and non-technical aspects of an organization for effective communication in handling potential security threats and other technical requirements. A CISO role has a significant responsibility to ensure the organization meets all requirements to minimize breaches in daily operations.

Any CISO needs to understand the legal compliance requirements that may apply to an organization. According to Diamond at Okta, some common compliance requirements in the U.S would be adherence to the Health Insurance Portability and Accountability Act (HIPAA), Defense Federal Acquisition Regulation Supplement (DFARS), Payment Card Industry Data Security Standard (PCI DSS), as well as other requirements if the organization is outside of the United States (Diamond, 2018). Organizations must meet compliance requirements to avoid hefty penalties and minimize the risk of a breach.

A CISO is also responsible for developing incident response (IR) plans for an organization. To develop an IR plan, a CISO needs to identify and assess internal and external threats, determine strategies for responding to said threats, and test the developed IR plan regularly to ensure its effectiveness. Developing an IR plan involves working with departments across the organization, and a comprehension of the underlying technological infrastructure within an organization and the role the infrastructure takes during a breach.

In the event of a cybersecurity breach, a CISO is one of the primary roles in responding to that threat. According to Hollenberger, a CISO is expected to provide the details of an incident to senior leadership as well as the respective IT teams so that those teams can perform their respective responsibilities during an incident (Hollenberger, 2023). The CISO also engages with legal to determine the implications of the breach. A breach for an organization can be a compliance nightmare and a public relation one. By having a CISO with excellent technical and non-technical skills an organization can reduce the footprint that a breach causes.

There are substantial requirements for anyone who wants to go into the Chief Information Security Officer. In addition to technical and non-technical skills, there is a strong desire to have industry certifications, such as the Certified Information Systems Security Professional (CISSP) certification (Whitman, 2021). By leveraging a CISO with proper qualifications and support, an organization could potentially see long-term cost savings by mitigating its risk.

**References**

Whitman, M. (2021). Principles of Information Security (7th ed.). Cengage Learning US. https://online.vitalsource.com/books/9780357506561

Smith, J. (2020). Cybersecurity Best Practices: A Comprehensive Guide. Publisher.

Anderson, M. (2019). Legal Compliance in Cybersecurity: Navigating the Regulatory Landscape. Journal of Cybersecurity.

(ISC)2 Cybersecurity Workforce Study, 2019.

InformationWeek, "The people who do and the people who watch shouldn't report to a common manager."

ISO 27001 posting on avoiding conflict of interest.

Meta Group survey on information security department positioning.

Charles Cresson Wood, "Information Security Roles and Responsibilities Made Easy."

SEC/CISE Threats to Information Protection Report, 2015.

Bureau of Labor Statistics (BLS) employment projections for information security analysts.

(ISC)2 Cybersecurity Workforce Study, 2020.

CyberSeek, cybersecurity supply/demand "heat map."

Diamond, J. (2018, April 3). *4 Compliance Regulations Every CISO Should Know*. Www.okta.com. <https://www.okta.com/blog/2018/04/4-compliance-regulations-every-ciso-should-know/>

Hollenberger, J. R., John. (2023, December 12). *What the SEC’s New Incident Disclosure Rules Mean for CISOs | CISO Collective*. Fortinet Blog. <https://www.fortinet.com/blog/ciso-collective/sec-new-incident-disclosure-rules-mean-for-cisos>

Whitman, M. (2021). *Principles of Information Security* (7th ed.). Cengage Learning US. <https://online.vitalsource.com/books/9780357506561>

Bowen, Hash, Wilson, P., Joan, Mark. (2006, December 1). Information Security Handbook: A Guide for Managers.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security*. Cengage.

Vacca, J. (2021). *Computer and Information Security Handbook.* Morgan Kaufmann.