ROLES IN CYBERSECURITY ORGANIZATION

Hannah Nirgin

[Institutional Affiliation(s)]

Author Note

[Include any grant/funding information and a complete correspondence address.]

# Introduction

Cyber Security is a big challenge in the current era of the advancement of Information Technology. Data has become one of the most important resources in the 21st century, and its protection and prevention from data theft and cyber-attacks is a major requirement for organizations. A cyber-security company is an organization dedicated to providing security solutions to organizations, including business firms, government organizations, security agencies, and also big enterprises. The security organization not only maintains the Security Operation Center (SOC) to monitor the security of the client's IT infrastructure and databases but also manages to prevent them from cyber-attacks and potential data theft. The risks of cyber-attack and related consequences can be minimized by building capabilities in three critical areas of detection, prevention, and response. In this paper, we will take a detailed overview of the organizational structure of a cyber-security company by explaining the roles of different positions and their links with each other.

# Chief Operating Officer (COO)

The Chief Operation Officer is at the executive level who has the duty to oversee all the operations related to the business of the organization. These operations or responsibilities are the management of human resources, vendor management, design management, production, and operations development. In Cyberworld, a very important factor is preparedness, so a COO is aware of new trends and requirements of cyber-security. This is done by an effective cyber literacy and incident planning of incident and response. A COO is responsible for handling all the issues, which may result in disruption of normal business operations of the organization.

It is part of the COO’s responsibilities to make sure continuity in the operations and functioning in crisis situations, including natural disasters, technology, or process change or economic shutdown(CyberVista, 2017). A COO ensures that cyber risk scenarios are configured according to the overall business and operational strategies. The plans for an incident response, which are developed by the Chief Information Officer, are also monitored by COO of the cyber company and implemented after his approval. In general, a COO protects the company by manipulating the cyber risk in the form of enterprise risk and enables the subordinates to practice the response plans.

# Chief Information Officer (CIO)

 In recent years, the role of CIO has become very important in cyber-security because of the induction of many complex exclusive IT processes and infrastructures in the field. The Chief Information Officer is in charge of a large part of technical and operational processes and makes sure that the right controls are placed for data integrity and security. The responsibilities of CIO in a cyber-security company are following

* The CIO focuses on the overall awareness as well as the training of cyber-security. This including providing services to facilitate the cyber awareness of application and analytic managers and that of the end-users.
* He is aware of the cybersecurity industry in term of the regulation which governs the industry. This is helpful in communicating the risks and postures to the necessary parties both externally and internally.
* It is the duty of the CIO to manage and enforce cybersecurity controls for vendors and also provide monitoring to maintain the business relationship.
* The CIO is responsible for implementing the frameworks like ISO and NIST and benchmarks the cybersecurity of the company appropriately(Stevens, n.d.).

Analyzing the role of CIO in emerging IT and cyber markets, the CIO is now majorly involved in the interoperation of frameworks and systems across the organization. This is mainly due to the inception of IoT (Internet of things) because greater connectivity is responsible for wider digital and communication systems.

Chief Information Security Officer (CISO**)**

The well-established duties of chief information security officers are repelling, monitoring, and then responding to the cyber threats by meeting requirements of the compliance. The CISO of a company is at the senior executive level in the hierarchy and is employed to deal with major implementation and to develop the information security infrastructures. The CISO often works closely with CIO to introduce services, develop products, and to manage plans of business continuity and disaster recovery. Talking about the qualification of a CISO, companies mostly prefer advance degree holders in the fields of computer science, engineering, and business. Apart from general degrees, relevant specific certifications are also required, including CISSP, ISACA, and ISC. Following are the responsibilities of a CISO in an Information security company.

* To make sure the fulfillment of the CIA is Confidentiality, Integrity, and Availability of information and resources.
* Doing a quick and real-time analysis of immediate attacks, risks, and threats.
* Communicating with the board and keeping them aware of potential security potentials and risks to enable them to make the right decisions related to business moves collaborations(Fruhlinger, 2019).
* To make sure that information is safe from internal human intervention.
* To make plans, purchase and implement the security-related software and hardware and ensure that the infrastructure meets the best security practices.
* To carry out efficient access management by making sure that only authorized persons have access to the systems and restricted data.
* To carry out forensics by doing penetration testing and enumeration and determine loopholes and vulnerabilities in the systems.
* To govern all the above-mentioned jobs to make sure smooth operation.

The other key responsibilities of a CISO are identifying C-level team members, embed information of security, create reports monthly, hire solid security staff, and strive to become an external and internal security expert.

# Chief Risk Officer (CRO)

A CRO is an executive at cybersecurity organization and has the responsibility to do the tasks of assessing and minimizing the significant regulatory, competitive, and technological threats to a business or enterprise’s capital. The officer is liable for the implementation of mitigation processes and operational risk management to avoid losses from failed or inadequate policies, systems, and processes. The risk management includes the development of IS processes, business disaster, and continuity recover planning and giving input on governing compliance regulatory data. The responsibilities of a CRO are following

* To develop strategic action plans and risk plans to mitigate the organization's primary threats and to evaluate the progress of risk minimization efforts.
* To disseminate and develop the risk analysis and to provide reports of progress to the organization's executives employees and other board members.
* Determining the risk appetite of the company and the amount of risk the company can take("What is chief risk officer (CRO)?" n.d.).
* To oversee budgeting and funding of mitigation projects and risk management.
* To develop and then implement risk assurance strategies and information for storage and transmission of information systems and data.
* Evaluation of potential risks due to system failure and employee errors that may result in business loss and developing the procedures and strategies to reduce those risks and respond in case of an attack.

For a well-reputed company, the qualification of a CRO is often post-graduation in IT, engineering, or business studies. It depends on the nature of the organization, but for a cybersecurity company, higher studies in the field of IT or information security are a must. Also, to demonstrate the need for strategic efforts to the stakeholders, strong communication skills are also required.

# Chief Finance Officer (CFO)

Generally, a CFO deals with the company's finances, but in the case of a cybersecurity organization, the role is a little more demanding. In fact, in an organization of such type, keeping information secure must be the priority of each employee. Experts in the field believe that information security is not a department; it is rather an attitude. CFO’s role in deterring and preventing an offense related to cybersecurity is important because company credits, purchases, and company credit cards are managed and processed under this position. Any hacker can break the barriers and cause harm to the company business. The key responsibilities of a CFO in a cybersecurity organization are following

* To understand the full risk universe of the organization
* To develop a close relationship with CIO and CISO.
* To do the evaluation of the insurance of the company’s cybersecurity.
* To provide timely reports to the board directors about the company’s new cybersecurity incentives (Gregg, 2010)
* To understand the related regulation of cybersecurity and expectations of the SEC, which have become very important these days from examination and reporting priority point of view.

Because of the importance of the CFO position in the organization, the employee must be well educated in the field of Information security, too, apart from qualification related to economics and business studies.

# Conclusion

To provide efficient and reliable security to the clients, the coordination among these roles is very important. As discussed above, the incident and response plans are monitored by the COO of the organization while CISO or CIO are responsible for the development and implementation of these plans and protocols. CRO and CFO are also required to work while maintaining the coordination with the higher management to ensure the smooth operation. By utilizing these positions efficiently, the risks of cyber offenses and related outcomes can be minimized to a great deal. To serve the purpose of ensuring confidentiality, integrity, and accessibility, all the officers discussed above must work in coordination by ensuring high standards of the security.

**References**

CyberVista. (2017, February 21). The Chief Operating Officer: Operate with Cyber Efficiency. Retrieved November 21, 2019, from CyberVista website: https://www.cybervista.net/chief-operating-officer-cyber-efficiency/

Fruhlinger, J. (2019, January 14). What is a CISO? Responsibilities and requirements for this vital role. Retrieved November 21, 2019, from CSO Online website: https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html

Stevens, M. (n.d.). Analyzing The CIO’s Roles & Responsibilities Regarding Cybersecurity. Retrieved November 21, 2019, from https://www.bitsight.com/blog/analyzing-cios-roles-responsibilities-cybersecurity

What is chief risk officer (CRO)? - Definition from WhatIs.com. (n.d.). Retrieved November 21, 2019, from SearchCompliance website: https://searchcompliance.techtarget.com/definition/Chief-risk-officer-CRO

Gregg, R. (2010). The CFO's role in managing cyber risk. *Financial Executive*, *26*(7), 61-63.