THE CHIEF INFORMATION SECURITY OFFICER (CISO) ROLE EXPLAINED

Information security is a top concern for business organizations, as research finds that cyber-attacks are launched 2,244 times a day—that's every 39 seconds. The average cost of a data breach is $3.9 million.

The role of Chief Information Security Officer (CISO) is gaining popularity to protect against information security risks. Let's take a look at the emerging CISO role.

What is a CISO?

The CISO is a leadership position responsible for:

- Establishing the right security and governance practices
- Enabling a framework for risk-free and scalable business operations in the challenging business landscape

However, a strong domain-specific technical knowledge and background is not critical to a successful CISO career. The leadership position is focused on understanding the security challenges in the current and future state of business operations, and to prepare the organization with the right tools, skills, resources, relationships and capabilities against growing information security risks.

The position of a Chief Information Security Officer (CISO) can take a variety of job tasks and

responsibilities depending on the size, hierarchy, industry vertical and compliance regulations applicable to the organization.

What are the responsibilities of a CISO?

The responsibilities of a CISO can spread across the following functional domains of the organization:

End-to-end security operations

A CISO must contribute to the design and approval of a comprehensive security strategy. The strategy will account for the end-to-end lifecycle of information security operations, including:

- Evaluating the IT threat landscape
- Devising policy and controls to reduce risk
- Leading auditing and compliance initiatives

The CISO brings onboard key stakeholders within the organization, secures the necessary funding and resources, and establishes necessary partnerships with external vendors and security experts. Finally, the CISO is expected to manage information security initiatives and employees across the

organization to ensure smooth transition toward security-aware and risk-free business practices.

Compliance

The CISO must ensure that their organization is adaptable to evolving compliance regulations. This is especially crucial for global organizations that must comply with a range of different regulations, and failing compliance can cost significantly—one such example is GDPR. The CISO develops the requirements for all interested parties and coordinates with the data protection initiatives in compliance with these requirements as per the enforceable regulations.

HR management

Recent research finds that more than half of all data breaches occur due to human error. It is therefore critical for the CISO to establish a system that reduces human error and its impact to their organization's security posture.

Responsibilities begin with setting the right criteria and mechanism to hire employees with knowledge and awareness of the security risks facing their daily work routine. These include, among others:

- Verification checks for job candidates
- Security education and training program
- Policies for identity and access management

Disaster recovery and business continuity

The CISO is responsible for resilience against cyber-attacks. According to a recent IBM research study, the average time to detect a breach ranges between 150 to 287 days, depending on the industry vertical. Once identified, containing a breach takes an average of 53-103 days.

Cyber resilience is not just about preventing and defending against information security attacks, but also recovering rapidly from security infringements. This is achieved by establishing a robust crisis communication channel, disaster recovery and risk management system. Every security breach incident and response activity should be analyzed. In this regard, the CISO is responsible for analyzing incidents and proposing improvements to the response strategy.

Documentation

The CISO contributes to a variety of security policy domains associated with:

- Compliance
- Governance
- Risk management
- Incident management
- HR management
- Additional domains

Teams and their managers routinely use documentation to follow security best practices and organizational policies in responding to security-sensitive business situations. Therefore, CISO must ensure that the documentation is up to date as per the current organizational policy. The

documentation and knowledge management activities should be designed to facilitate convenient access of information and contribution with new information in the form of reports, employee feedback or other insights generated across the organization.

Stakeholder onboarding

Security initiatives often require significant financial and workforce resources, which can emerge as a conflicting goal against stakeholders pursuing maximum business returns. The CISO is responsible for evaluating business opportunities against security risks that can potentially compromise long-term financial rewards. The CISO defines an optimal tradeoff between the opportunities and risks associated with information security projects that would protect long-term growth of the organization.

For this purpose, onboarding top management executives is crucial. Regular notifications and updates to other business leaders, proposing optimal budgeting strategies, and the role of ongoing security initiatives against security risks is therefore a routine activity for a CISO.

Additional CISO roles and responsibilities

In addition to these key responsibilities, a CISO can take on a diverse set of challenges that follow within the scope of a technical and non-technical scope their role, including:

- **Contributing to technical projects.** These can include system design and architecting layers of security against potential attacks.
- **Partnering with internal and external providers.** These can include executives and managers across different departments, third-party vendors, government institutions and thought leaders in academia and the wider industry.
- **Evaluating employee behavior and organizational culture.** These include preventing the situation where an employee goes rogue due to toxic work culture, reviewing and recognizing suspicious behavior, and ensuring a fair work environment for everyone.
- **Financial reporting and addressing cybersecurity as a business problem.** A security initiative may not always be worth the financial investment. The CISO is expected to produce the best outcome both from a security and a business perspective, without compromising regulatory compliance, end-user privacy, and user satisfaction.

The CISO, the CIO, the CTO

In small organizations, these responsibilities of a CISO may be delegated to a Chief Information Officer (CIO) or a Chief Technology Officer (CTO) instead of creating a separate CISO position. These executives are responsible for navigating security well ahead of potential security incidents as their organizations scale rapidly and embrace new digital transformation initiatives. They should be aware of their organization's security strengths and weaknesses, and help it adapt before a security incident can cause any significant damages.

Additional resources

To learn more about cybersecurity and leadership roles, check out the BMC Security & Compliance Blog or browse these articles:

- Cybersecurity: A Beginner's Guide
- How CISOs should navigate security in the months ahead
- Solving the Security Risk Your CISO Doesn't Know About
- 4 Essential Leadership Qualities