RISK AND ITS PLACE IN THE EVER CHANGING ROLE OF SECURITY

AN OPTIV VIEWPOINT

Just as information technology priorities change year after year at most organizations, so should the way we view the security landscape. To best address the constant shifting, organizations must realign and reorganize. Over the past five years the role of the Chief Information Security Officer (CISO) has changed dramatically. Organizations need to observe the evolution of the role of the CISO and transform the skills and priorities to meet the demands of the new role. The focus is no longer just on information technology, but also, on a broader set of priorities that reflect the different way organizations operate. Security is no longer an IT problem, it is a business problem and the role of the CISO needs to adjust to these changing needs. At the foundation is the focus on risk to information regardless of its form or location. Because of the new requirements of a security leader, we must consider changing the way we think about Initially the CISO was solely focused on protecting the information technology systems and the data on those systems. Now, we must focus on managing the risk associated with our data, rather than just how we're protecting it. The question then remains, what are the requirements of a successful CISO today?

A CHANGE IN RESPONSIBILITY

To focus on who is managing asset risk, we typically look to the Chief Information Security Officer, or CISO, of an organization. This position is typically viewed as a technical role, coming up through the ranks with an IT background and then moving into security. Their main job function has historically been the implementation of security technologies within the organization, with an emphasis on the infrastructure and keeping the internal systems secure. As the "S" in CISO implies – the focus was on security.

Over the past few years, the responsibilities of the CISO have expanded beyond the security of the enterprise. Now, the role must concentrate on managing the risk of the information, regardless of where it resides. Today's CISO has evolved into the Chief Information Risk Officer (CIRO), with a growing list of responsibilities – including all or some of the below, depending on the industry and company demographics.

Information Risk Management
A CIRO needs to understand all aspects of threats to the organization's information and business operations.

The security strategy should be focused on enabling the business and minimizing the risk to the information.

OPTIV

Regulatory Compliance Management
Almost every industry is subject to a set of industry specific security and privacy regulations, and most large companies operate businesses outside the US with their own regulatory requirements. The CIRO needs to understand the laws within the jurisdictions they operate, working with their legal and regulatory compliance teams to implement the necessary protections and processes to demonstrate compliance with the law.

Third-Party Risk Management
It is important for a CIRO to identify the information that is flowing outside the organization and the third-parties that provide services impacting business operations. The proliferation of outsourcing and cloud providers has made this responsibility more critical than ever. The CIRO must be able to establish a process for measuring and managing the risk of these external entities and quantify that risk to the overall business.

Business Acumen
The CIRO must have a keen understanding of technology and be an excellent communicator in business terms. They need to be able to translate the complexities of the entire security ecosystem into a language that executive leadership and board members understand. Their success is measured by their ability to communicate the organization's current level of information risk and how it is managing the risk over time, putting security and privacy projects into terms of value to the organization.

For most organizations it is not a matter of "If" they have a security breach it is a matter of "when". Over the past few years there have been major security breaches that lead to disclosure of sensitive information. The cost of the breach to the organization is greatly dependent on their ability to react to the breach in timely and efficient manner, and then communicate to the regulators and public on what occurred. The CIRO not only focuses on the protective controls but also puts an emphasis on being prepared for a breach to detect, eradicate and then respond. The business acumen skills are need to be successful at minimizing the damage done to the reputation of the company and the long term impact of the breach.

There will be a growing number of CIROs in the future, with a mission to manage the information risk of the organization across all aspects and locations. For many companies, the position of the CIRO is moving out of IT and more in line with the other "C" suite roles. Now the question is, where does this new CIRO position fall within an organization's reporting structure?

THE EVOLUTION OF SECURITY STRATEGIES

The shift from CISO to CIRO leads to discussion on structuring reporting relationships that support both open communication and collaboration between the CIRO and other areas of the business. Equally important is the CIRO's responsibility to keep the board of directors informed of the risks the company is facing from security, privacy and regulatory threats.

Depending on company size, industry sector and security program maturity, many different security strategies are deployed across organizations today. The evolution of IT-based security programs, to compliance-based, to now threat and risk-based security programs illustrate the journey organizations take as their security programs mature and move toward a business-aligned program.

IT-Based Security Program

This traditional approach focuses on the implementation of security technologies within the organization. The function of security is seen as a component of the IT team. The emphasis is on the infrastructure and keeping the internal systems secure.

Compliance-Based Security Program

Organizations that are highly regulated focus their efforts on complying with security and privacy regulations. This is the most common program seen today; however, recent security events have shown that compliance does not equal security and it alone is not an effective strategy.

Risk-Based Security Program

The best security programs are business-aligned. It is critical for organizations to understand the goals of the company and recognize the threats they face that hinder those objectives. Organizations face different threats based on specific attributes. For example, a

highly public-facing organization will have a greater likelihood of a DDoS attack than others, while organizations with significant size and complexity will have a larger probability of an advanced persistent threat (APT) attack. Combining the business goals, risks and threats is the key to developing a highly effective information risk program.

As organizations move toward this risk-based security approach, the CIRO will have many responsibilities that are not directly related to information technology. This is why it is necessary to shift away from the traditional reporting structure (where the CISO reports to the CIO) so that the CIRO is in a position to communicate directly to the board and other key executives in order to support the ongoing information risk management of the organization.

INFORMATION RISK MANAGEMENT SHIFT

There is no silver bullet when it comes to the "right" organizational structure, but I have found that some approaches are more successful than others. For each unique organization, the primary considerations are the size, corporate culture, industry sector. Lately, there has been a trend to move security out of the IT department and into a reporting structure that supports the ongoing risk management of the organization. The mission is no longer to only secure the data, but to now manage the risk the data is presenting. Traditionally, the CISO has reported directly to the CIO. Figure 1 below shows this reporting structure.

Figure 1 – Traditional CISO Reporting Structure

In this model, security operations fall under the CISO. As a technical function, the role includes security architecture, technology systems integration, configuration, vulnerability management and monitoring. This focus on deploying and managing technology is contrary at times to managing information risk. The role of the CIO is to deploy technology systems and the role of the traditional CISO is to focus on protecting the information – this can cause a natural conflict of interest between the two leaders. It is a good practice for organizations to divide the responsibilities for managing operational availability from managing information security.

To overcome these challenges, a new model has emerged that breaks down the different roles of the security team and provides lines of communication so that the right individuals can be informed and consulted, and actions can be made to lessen information risk. Figure 2 below illustrates the emerging CIRO reporting structure.

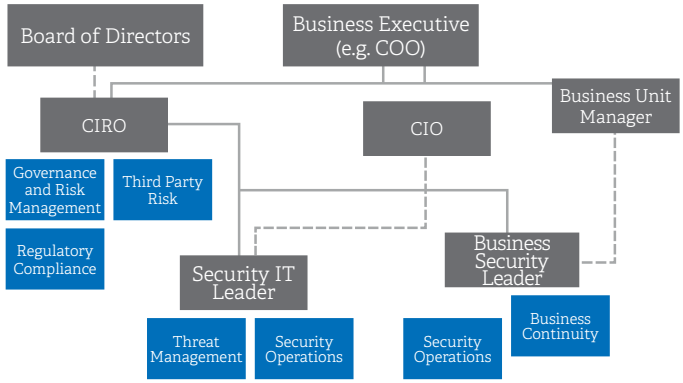

Figure 2 – Emerging CIRO Reporting Structure

In this model, there are additional responsibilities for third-party risk and regulatory risk management under the CIRO, illustrating that they are accountable for managing the risk of the information regardless of where it resides. This is also different from the traditional model in that the CIRO is a key member of the executive staff and has a direct line of communication with the board. The roles of the security team are also broken out in this model:

CIRO – specializes in translating business initiatives into security and risk management requirements and programs that must be implemented to support the corporation's goals and objectives; collaborates with the executive team to ensure timely and appropriate progress; communicates to the board the current information risks facing the organization and how those risks are being managed overtime; manages the Security IT Leader and Business Security Leader.

Security IT Leader – focused on technical security issues including security architecture, engineering, and security operations and monitoring, network and web application firewalls, intrusion prevention, data leakage and other security technology systems; manages the technical security requirements such as configuration and vulnerability management; responsible for scanning networks, systems and applications for vulnerabilities; has a direct line of communication to the CIO to collaborate with the IT team.

Business Security Leader – concentrates on the business requirements and enables the business to meet their objectives; acts as the liaison between the business and the information security group; responsible for the overall compliance of the business to the established security policies and requirements; ensures that projects within the business have integrated security so there are no delays when implementing new initiatives; coordinates with IT Security Leader about any security implementations, performs audits or penetration tests of business assets; has a direct line of communication to the Business Unit Manager so that security is a priority in every line of business within the organization.

Depending on the company culture, business structure and other factors, the model can also be modified so that the Security IT Leader reports directly to the CIO and/or the Business Security Leader reports directly to the Business Unit Manager. Either way the responsibilities remain the same and the important factor is having the communication and collaboration between the different groups mapped out as seen above.

Some of the major benefits of this new model over the traditional are that it:

- Aligns the information risks with the business priorities;
- Supports the shared responsibilities of information risk (information security is not a IT problem, it is a business problem); and,
- Includes the full spectrum of information risks that organizations are facing today and provides a reporting structure to gain visibility and implement the strategy.

I do not claim that the above model is a one-size-fits-all, but it does give a general layout of how to structure an effective information risk management approach. When implementing a version of this structure to your own organization my recommendations are to:

Start Slow	Start Now
First align the reporting structure to meet the needs of the business, and then add the additional responsibilities of the full suite of information risk over time.	The material risk of information to the corporation has never been higher and doing nothing is not an option.

BEGIN MAKING CHANGES NOW

The role of the information security officer is changing, but like all major shifts in culture and organization, this transformation will not happen overnight. As organizations move toward this risk-based security approach, the CIRO will have many responsibilities that are not directly related to information technology. Besides the shift in the CISO to CIRO role, organizations should consider a model that includes a Security IT Leader and a Business Security Leader to help keep security a priority within every part of the company. Though this is by no means a one-size-fits-all method, it can lead to a more effective risk management approach. Along with aligning information risks with business priorities, the shift toward this role structure supports the shared responsibilities of information risk and includes the full spectrum of threats that organizations are facing today.

> The material risk of information to the corporation has never been higher and doing nothing is not an option.

When security leadership with the proper skills work within a structure that supports their success, the organization is better positioned to level the battle field against threat agents and protect their company from attacks.

James Christiansen
CISO

1125 17th Street, Suite 1700
Denver, CO 80202
800.574.0896
www.optiv.com

Optiv is a market-leading provider of end-to-end cyber security solutions. We help clients plan, build and run successful cyber security programs that achieve business objectives through our depth and breadth of cyber security offerings, extensive capabilities and proven expertise in cyber security strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.

4.18 | F2