CYE

The Changing Role of the CISO from IT Leader to Business Enabler

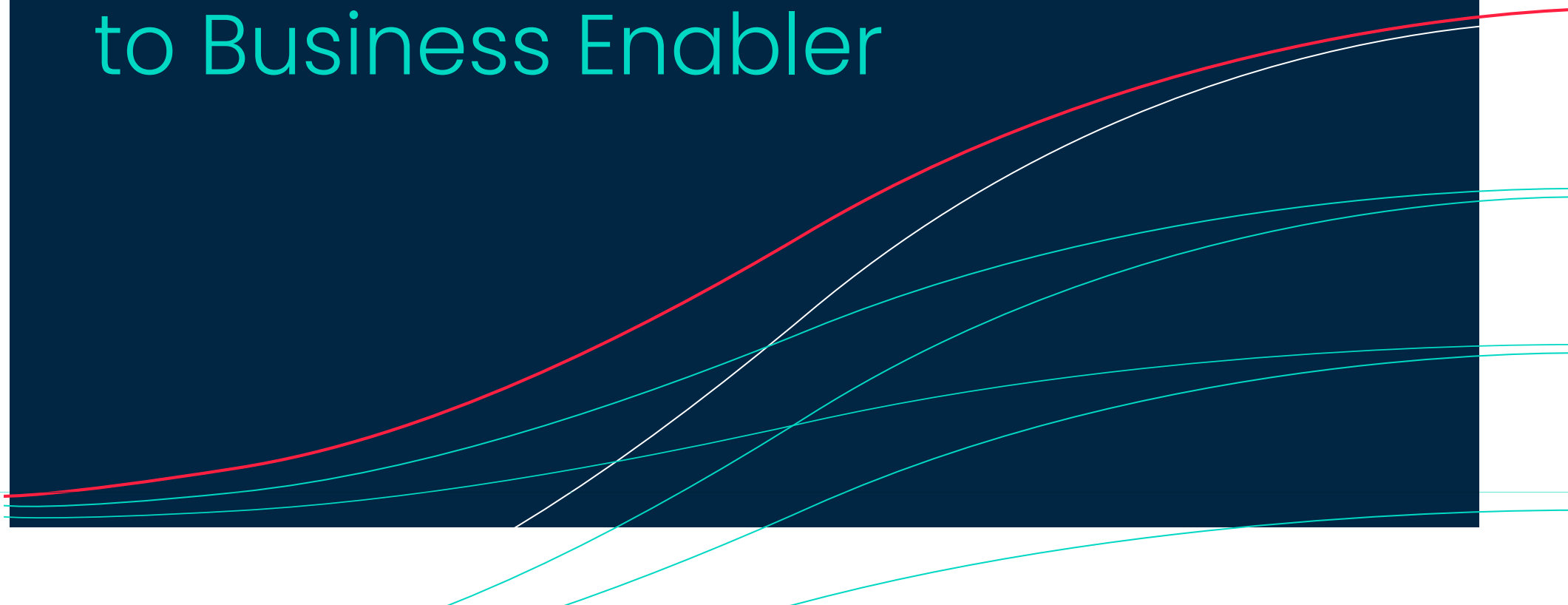

Table of Contents

What is a Chief Information Security Officer?	Page 3
The Evolution of the CISO Role	Page 4
The CISO Evolution Timeline	Page 5
CISOs in the Past and Today	Page 6
The Challenges Faced by the Modern-Day CISO	Page 7-8
The Top Qualities of a CISO	Page 7
The Many Roles of the Modern-Day CISO	Page 9
The CISO Role: Next Steps	Page 10
How CYE Can Help CISOs	Page 11

What is a Chief Information Security Officer?

In all sectors and across most geographies, organizations are rapidly widening and deepening their reliance on digitization. Alongside the growing reliance on technology, companies are increasing their dependency on data to generate better service and offer greater value to customers.

Roles such as chief data officer, chief technology officer, and chief innovation officer are just some of the new functions organizations that rely on technology and data have added to their executive teams. Chief information security officer (CISO) is another such role, which most companies can no longer do without. The CISO role is quickly gaining momentum not just as a technology function, but as a business one.

The CISO is the executive responsible for protecting an organizations' digital assets, intellectual property, and data. At its simplest, the CISO is the head of IT security. However, in modern organizations, the CISO's responsibilities extend beyond mere security operations to encompass the enterprise vision as well. The modern-day CISO is expected to balance security needs with business goals and align the organization's security program with overall business strategy.

The Evolution of the CISO Role

The first CISO role dates back to 1995, when the banking corporation Citigroup suffered a series of cyberattacks, leading it to develop the world's first cybersecurity executive role. Widespread adoption of the chief information security officer role began in the late 1990s and early 2000s, as organizations began to recognize the need to protect their digital assets.

In the beginning, the CISO's responsibilities were mostly IT related and focused on implementing firewalls, intrusion detection systems, and other security technologies. CISOs were responsible for these systems' configuration and maintenance, and for ensuring that security policies were applied.

As companies underwent digitization, increasing their reliance on IoT, cloud, and mobile technologies to grow their business and run their operations, their attack surface widened. The CISO was forced to learn how to secure a wide range of environments, domains, and premises, and deal with much greater volumes of cyber risk.

This was not the only change CISOs needed to overcome. Organizations' increased reliance on technology and data meant that CISOs had to develop security plans that offered protection without slowing down or impeding business goals. CISOs became less narrowly focused on technology and more broadly focused on finding solutions that would align with business objectives.

Today's CISOs are first and foremost part of the organization's executive team. They are expected to frame security problems and their solutions in terms of business impact and develop frictionless and seamless security plans that work in tandem with the business goals.

The CISO Evolution Timeline

1980s

The concept of computer security is first introduced.

1990s

The CISO role emerges and is first seen at Citigroup and shortly after at Motorola Inc.

2000s

The CISO role expands to include a wider range of responsibilities such as risk management, compliance, and data privacy.

2010s

The CISO role becomes critical as high-profile cyberattacks such as the Target breach draw attention to cybersecurity. CISOs are also expected to display expertise in emerging technologies including cloud computing, IoT, and AI.

2020s

The CISO is seen as a key player in organizations' digital transformation and is included in the C-suite. CISOs are expected to align security protocols with business objectives. The role also becomes more collaborative, working closely with other departments such as legal and compliance.

CISOs in the Past and Today

	CISOs in the Past	CISOs Today
Strategic focus	Technical security	Aligning security goals with business goals
Reporting to	Technical managers and IT executives	Management and board of directors
Risk Management	Narrow focus on IT systems	Broad focus on all company systems, platforms, environments and devices, on-premises and remote
Security Tools	Multiple firewalls, threat detection systems, and other security technologies	Consolidating security services to an all-in-one security solution
Communication	To direct managers who are fellow technology professionals	To C-suite and board members who don't necessarily have a technological background. Also laterally and downwards to educate, train, and implement security protocols

The Challenges Faced by the Modern-Day CISO

CISOs have had to adapt their security strategies to align with new technologies, new work models, and a constantly changing threat landscape. These are the main challenges they face:

1. Managing Technologically Complex Environments
Companies leverage a wide range of technologies to achieve their business goals and maintain their competitive edge. CISOs and their security teams are expected to have a deep understanding of these technologies and the risks associated with each one of them. CISOs are then required to devise security plans that align with these diverse technologies and offer protection across all the company's domains and premises.

2. Remote and Hybrid Work Models
The shift to remote work has led to an increase in the use of personal devices for work purposes, which has created a significant challenge for CISOs and IT departments. These devices may not have the necessary security software installed, or they may not be configured to meet the organization's security standards. This can leave the company's data and systems vulnerable to cyber threats such as malware, phishing attacks, and data breaches.

3. Managing an Evolving Threat Landscape
Cybercrime is dynamic and ever-changing, requiring that the CISO continually adapts security strategies to keep pace with the evolving threat landscape. This requires ongoing threat detection, continuous risk assessment, and the manpower to analyze and report new vulnerabilities. CISOs may struggle to find the bandwidth and manpower need to ensure they are not caught off guard.

The Top Qualities of a CISO

- Be a leader
- Have a broad, company-wide, vision
- Be business-focused
- Be a problem-solver
- Be a strategic thinker
- Have a strong risk tolerance
- Be adaptable
- Be able to communicate upwards to management, as well as laterally and downwards across the organization with appropriate messaging for each audience

Ultimately, a successful CISO should possess a combination of technical, leadership, and business skills, as well as a deep understanding of the organization's goals and plans.

4. Being "On" at All Times
Cybercriminals don't keep regular office hours and are always on the lookout for new ways to be attacked. This means that threat management and incident response must be a round-the-clock effort. However, staffing a 24/7 security team can be a challenge, especially for smaller companies that don't have the budget to support it. CISOs are expected to have a response strategy in place that covers all hours of the day, and they must have the manpower to execute it.

5. Budgetary Constraints
Data breaches are costly when they happen, but if the company has not yet experienced the effects of an attack, this may be difficult to explain to management. With today's decreasing budgets, CISOs will need to justify the cost of security and may encounter pushback from management when requesting budgets. Security leaders need to know how to communicate with management effectively, translating technical security terms into business terms, and correlating security threats with their effect on business.

6. Shortage of Qualified Talent
As the demand for security professionals grows, positions can be hard to fill. The shortage of security talent may make it harder for CISOs to find and afford security professionals who are proficient in all the different technologies, and have the experience and expertise needed to carry out elaborate security plans effectively and responsibly.

7. Alert Fatigue
CISOs are at risk of overburdening and burning out their teams with high volumes of security alerts coming from the multiple security solutions they use. CISOs must remain vigilant about responding to critical alerts, while not letting the stress of ongoing notifications distract them.

8. Impact of Security on the Business
CISOs are expected to devise security plans that work seamlessly with the business operations. The requirement for frictionless, scalable security measures that align with business goals may be challenging to achieve.

The Many Roles of the Modern-Day CISO

The CISO is primarily a security and IT professional, but today's CISO also takes on leadership roles, educational functions, project management duties, and more. Here are some of the different hats a modern-day CISO must wear:

The CISO as a Cross-Organizational Security Expert
One of the main responsibilities of the modern-day CISO is to develop and implement a cross-organizational security strategy. Once a security plan is ready to go, the CISO must work closely with different departments to ensure that the plan is integrated successfully. This may include working with the legal team to ensure compliance, the HR department on employee training, or partnering with the IT team to introduce new security tools.

The CISO and the security team will explain, educate, and train employees across the organization, from different departments and teams, both technical and not, about the security plan. The CISO will deliver security information to different audiences, with varying levels of technological background and security proficiency, and is expected to adjust security training to the different audience groups.

The CISO as an Executive Role
In addition to technical duties, the CISO also plays a key role in business decisions. The CISO is tasked with making security decisions that align with overall business goals.

The CISO must present security findings to management and board members, defend the security plan, and request the budget needed. To do this, the CISO uses cyber risk quantification tools that correlate security risks with their impact on the business. The CISO then uses this data to present a clear picture of the organization's security posture, the risks it faces, the potential cost of an attack, and what it will cost the company to reduce these risks. By approaching management with a set of datapoints that "speak their language," the CISO can involve the executive team in the company's security.

The CISO as a Thought Leader and Influencer
The CISO serves as the face of the organization for the media, customers, potential clients, and the security community. As a security expert and ambassador of the company, the CISO is expected to be well-versed in security current events, and able to share expertise as a thought leader and an influencer.

The CISO Role: Next Steps

1. CISOs and the organizations they work for must first understand the new responsibilities placed on the shoulders of security professionals.

   These responsibilities have evolved dramatically from what they were even a few years ago and will continue to change as new security challenges come to life and new defenses become necessary. Specifically, today's CISOs face a much vaster threat landscape, and are required to defend a much bigger attack surface.

2. CISOs must then take stock of the security tools and services the organization uses and assess their effectiveness and their ability to work cohesively with each other. While security tools may offer good defensive capabilities on their own, they may not integrate well with each other, creating clutter and chaos, and ultimately burdening the security team.

   In recent years, CISOs have been reducing their reliance on multiple security tools and services and moving to all-in-one solutions that streamline security processes, increase visibility across the organization, and work smoothly to achieve the best security posture possible.

3. CISOs should strive to find security solutions that offer both defensive and offensive capabilities. Their plans should follow the three steps to security maturity: cyber risk assessment, a quantification process that correlates the cyber risks the company faces with their cost to the business, and a mitigation plan that reduces that risk.

4. Once an organization's security risk is at a comfortable minimum, CISOs should ensure they have an incident response process in place that can be executed immediately in case of an attack.

5. CISOs should also get comfortable with having a seat at the executive table. They should take steps to translate technical considerations into business terms and visualize the organization's security situation in a way that resonates with management.

How CYE Can Help CISOs

CYE has developed a unique set of offerings that combine technology and human expertise to answer the complex needs of the CISO role.

CYE's Hyver platform is the only technological solution on the market today that combines attack route visualization capabilities with a cyber risk quantification functionality to help CISOs in their communication with management. The platform's visualization capability allows CISOs to see the potential impact of each vulnerability on the company's assets and implement a mitigation plan that prioritizes accordingly. This is critical to planning ahead and creating a manageable, sustainable security plan that reduces alert fatigue and early burnout.

Hyver's ability to pinpoint vulnerabilities found across all the organization's domains and premises is extremely useful to CISOs operating in today's technologically abundant environments. With Hyver, CISOs can gain visibility into all environments, from OT to IT, from on-premises to remote devices, and the cyber gaps detected at each level.

Hyver's cyber risk quantification allows CISOs to translate cyber risk into business risk, putting the security risks the company faces into monetary terms that management understands.

CYE's CISO advisory services are the human capital addition to the Hyver platform, giving organizations access to world-class security advisors. CYE's experts are highly experienced in all security aspects, supporting teams with day-to-day managerial tasks such as mitigation prioritization and patching, as well as long-term strategic planning, risk reduction, and ongoing mitigation roadmaps. CYE's expert security advisors are also trained to build ready-to-execute response plans that can be put to use immediately in the event of an attack.

Finally, CYE's assessment and red teaming services are available to CISOs who may not have the in-house capabilities to execute these extensive checks or would rather outsource the arduous task of uncovering the organization's threat landscape to seasoned professionals.

© 2023 CYE, All rights reserved. www.cyesec.com | info@cyesec.com

Want to learn more about how CYE can help CISOs?

Contact us