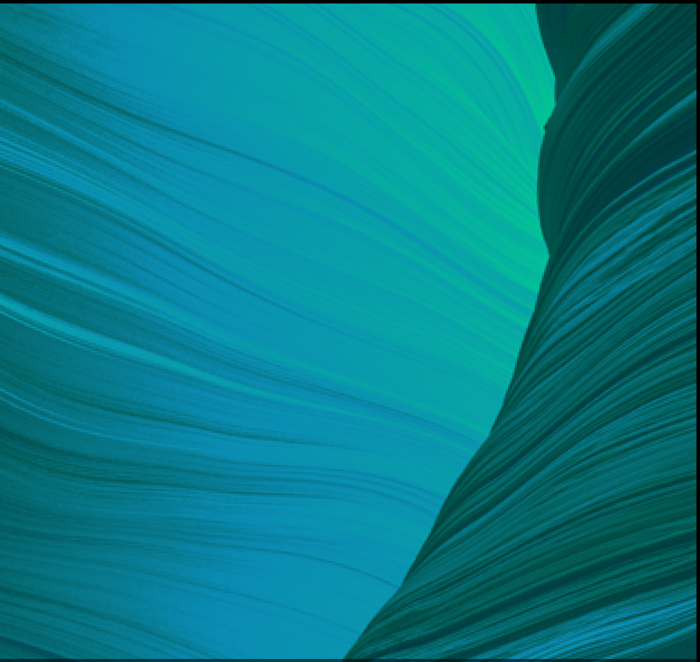
Essential strategies for CISO success in the first year

EY Center for Executive Leadership

The better the question. The better the answer.
The better the world works.

EY

Shape the future
with confidence



Contents

Evolving role of the CISO

Many paths lead to the chief information security officer (CISO) chair today. The position can serve as both a career pinnacle and a stepping-stone to other executive roles. As the cybersecurity landscape continues to evolve and grow in importance, a CISO can expect to face unprecedented challenges and opportunities in the role. Because CISOs have varying backgrounds and come into organizations with different challenges, the best course of action will be unique to each CISO and based on the organizational constructs the CISO operates within. However, a well-defined plan for your first year as a CISO can help you achieve milestones that are important for protecting your organization and amplify your personal impact.

There has never been a more pivotal time to be a CISO. While traditional responsibilities such as risk management, compliance and incident response remain core to the role, CISOs are increasingly involved in corporate strategy, IT governance, data privacy and supply chain security – all vital in today's disruptive environment. Research from Ernst & Young LLP (EY US) confirms that cybersecurity remains center stage: 84% of C-suite leaders say their organization's focus on cybersecurity has increased compared with three years ago. What's more, 85% also say their organization's cybersecurity focus will increase over the next year compared with today. Not only will cybersecurity continue to be a key focus area for the executive team and board of directors, but CISOs also take on significant personal responsibility in the role. The CISO is one of the few roles in the C-suite that is held personally liable for failing to protect the organization.

CISOs are increasingly sought-after executives, and those who effectively align cybersecurity with business objectives are sometimes groomed for broader leadership roles in technology. From the start, you will need to manage numerous demands right away: Instilling confidence, defining your vision, articulating your strategic goals and building a cohesive team will all be essential boxes to check during your first year.

Our one-on-one CISO program has assisted numerous executives over the past few years in successfully transitioning into the CISO role by defining priorities, creating strategic roadmaps, connecting CISOs to peers and enhancing skills in critical areas. We've identified five broad groups of key actions that successful CISOs typically pursue in their first year, complemented by tactical suggestions in the CISO checklist at the end of this article, that can guide your personal journey as you transition into the role and pave the way for your future career aspirations.

1 Review your current state security posture across the organization

An independent assessment of the company's cybersecurity posture, including policies, procedures and technologies, is an important first step, even for CISOs who are promoted from within and already possess deep institutional knowledge.

In today's rapidly evolving threat landscape, it is imperative for CISOs to conduct a comprehensive review of the current state of the organization's security posture. This involves assessing existing security measures, identifying vulnerabilities and verifying compliance with applicable regulatory requirements. By leveraging advanced analytics and threat intelligence, CISOs can gain actionable insights into potential risks and develop a robust strategy to mitigate them.

Once the assessment is complete, you should identify enhancements to the security posture that align with the organization's strategic objectives. This should include clear policies and procedures, key performance indicators (KPIs), and processes. Based on the desired future state of your cybersecurity function, the following are a few things to keep in mind:

Identifying areas for improvement, both quick wins and over the long term, can instill a sense of confidence in a new CISO.

Prioritizing a proactive approach to security will empower CISOs to protect the organization against emerging threats and promote enterprise resiliency.

Regularly updating security protocols and conducting penetration testing will not only safeguard sensitive data but also build trust with stakeholders.

Engaging with cross-functional teams enhances collaboration and fosters a culture of security awareness throughout the organization.

Common CISO challenge: Building and leading a high-performing security team is a significant challenge for new CISOs. They must assess the skills and capabilities of their team members, identify gaps, and foster a culture of collaboration and continuous improvement.

2 Build trusted relationships with key stakeholders

The importance of building trust and social capital with key business leaders across the organization cannot be understated.

The effectiveness of a CISO is significantly influenced by their ability to build strong relationships with key stakeholders across the organization and their ability to build and execute a strategy that is aligned with the rest of the enterprise. CISOs must understand the organizational strategy (including but not limited to the approach to growth of the business in the form of new products and/or expanded markets, mergers, acquisitions, and divestitures) and design a cybersecurity program that supports that strategy.

Without this, CISOs run the risk of being viewed as a technologist or having business leaders view cyber as a pure technology issue. But cybersecurity is indeed a business issue. EY analysis shows a direct correlation between share price declines and cybersecurity breaches. Companies are seeing real costs associated with cyber incidents, with a longer impact than envisioned.

Common CISO challenge: CISOs must balance the "duality of security": the need to protect existing infrastructure while innovating to support new business initiatives in line with broader organizational growth goals and strategies.

Successful CISOs invest the time to understand the business and, in turn, ask that business leaders understand the topics and business implications of cybersecurity and resiliency-focused risks. Just as CISOs ask that the whole organization understands cyber, CISOs should endeavor to understand what their counterparts do. It's important to establish relationships with frontline business unit leaders and other key stakeholders, such as the chief risk officer, chief marketing officer, chief human resources officer, chief legal officer, head of procurement, IT department, internal audit, compliance officers and other relevant personnel.

While getting to know these people, take the time to understand their perspectives on cybersecurity and their expectations of you. Help them understand cybersecurity by sharing compelling examples and the "so what" rather than overly technical details. More likely than not, there will come a time when you must ask a favor of your colleagues. Make the time and social capital deposit up front so you can take out withdrawals down the road.

Don't forget that cyber is one of the hottest topics in the boardroom. Understand the expectations of the board and oversight committee members, develop a communication cadence and reporting package that addresses key risks, and establish a strong working relationship with the chair of the audit committee or other key committee designated with cybersecurity oversight.

Common CISO challenge: Despite CISOs overseeing one of the most critical risks to organizations, their rank and influence often do not reflect the importance of their responsibilities, and they are often further down in the organizational hierarchy. There is often a disconnect between the CISO and their C-suite peers regarding the organization's level of preparedness to defend against cyber threats. CISOs must find effective means to influence peers and obtain the necessary budget to protect the organization.

Board-level committee oversight*	2024	2022
Disclosed that at least one board-level committee was charged with oversight of cybersecurity matters*	95%	89%
Disclosed that the audit committee oversees cybersecurity matters	81%	72%
Disclosed oversight by a non-audit-focused committee (e.g., risk, technology)	29%	28%
Disclosed oversight by a risk committee	13%	11%
Disclosed oversight by a technology committee	10%	9%
Disclosed oversight by another committee (e.g., compliance)	8%	8%

*Some companies delegate cybersecurity oversight to more than one board-level committee.

Source: "Cybersecurity oversight disclosures: what companies shared in 2024," EY Center for Board Matters, 15 October 2024; Fortune 100 companies, 2024 proxy statements.

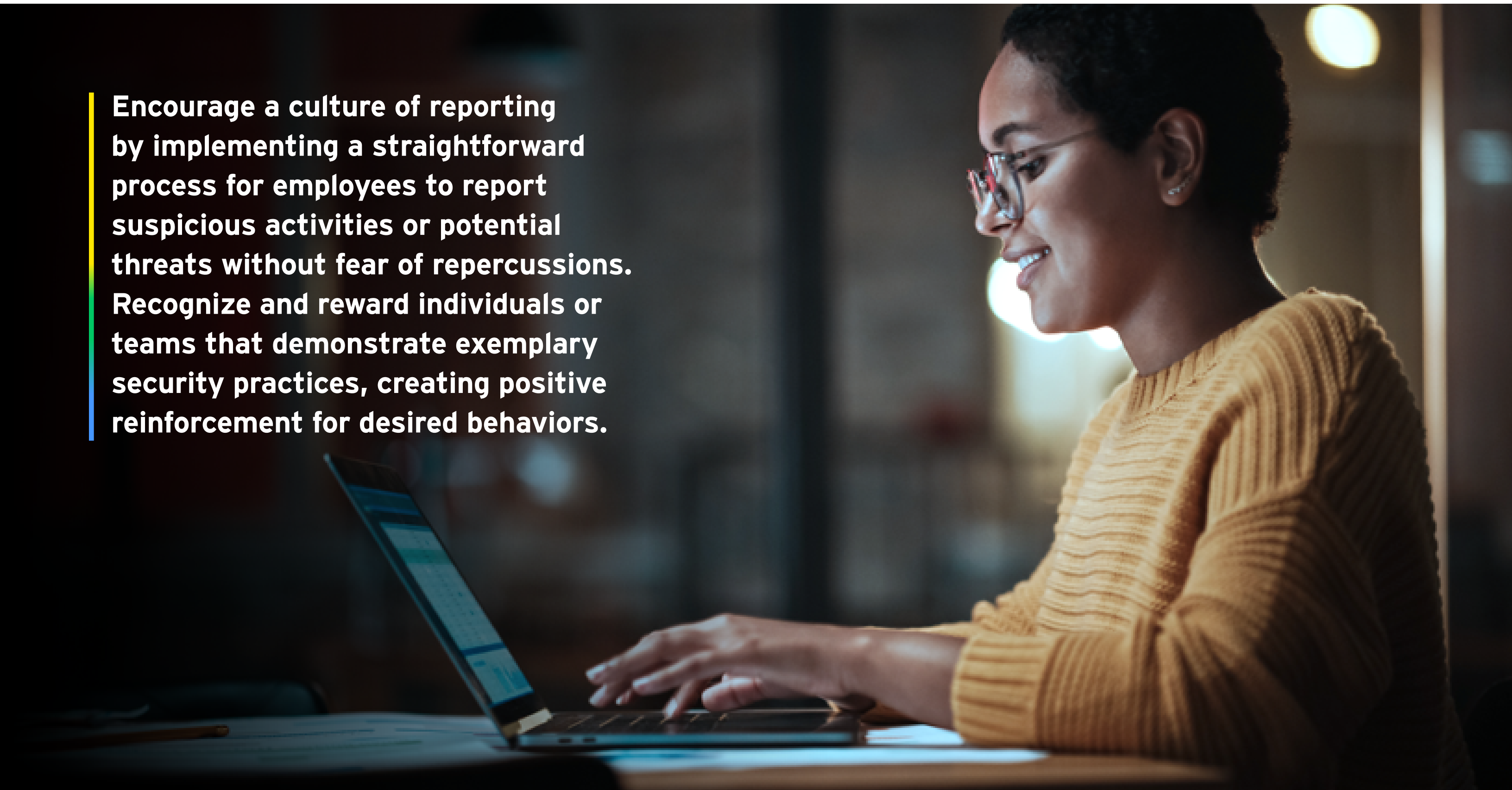
3 Enhance culture and awareness

Cybersecurity is a collective responsibility that extends beyond the cyber team. It involves every director, employee and third-party provider.

CISOs are increasingly taking a leading role in driving digital transformation initiatives, enhancing security posture and fostering a culture of cybersecurity awareness throughout the organization, highlighting the expanding scope of their influence. Building a culture of cybersecurity awareness within an organization starts with your leadership commitment and your ability to clearly communicate your vision, while also showcasing your understanding of the organization's larger growth strategy. As a new CISO, it's essential to lead by example and demonstrate the importance of cybersecurity in every aspect of the business.

Develop a comprehensive training program that is engaging and tailored to different roles within the organization. Utilize various formats, such as workshops, e-learning modules and interactive simulations, to cater to diverse learning preferences. Regularly communicate the significance of cybersecurity through newsletters, town hall meetings and internal communications, emphasizing that everyone plays a crucial role in protecting the organization. As risks and attacks continue to increase in frequency and complexity, understanding and guarding against cyber risk is critical.

In addition to formal training, fostering an open environment where employees feel comfortable discussing security concerns is vital. Encourage a culture of reporting by implementing a straightforward process for employees to report suspicious activities or potential threats without fear of repercussions. Recognize and reward individuals or teams that demonstrate exemplary security practices, creating positive reinforcement for desired behaviors. Incorporate cybersecurity into the organization's core values and mission, so that it is viewed as a shared responsibility rather than one that is solely owned by the IT or security teams. By consistently reinforcing the importance of cybersecurity and making it an integral part of the organizational culture, you can empower employees to take an active role in safeguarding the organization against threats.



> **Encourage a culture of reporting by implementing a straightforward process for employees to report suspicious activities or potential threats without fear of repercussions. Recognize and reward individuals or teams that demonstrate exemplary security practices, creating positive reinforcement for desired behaviors.**

4 Elevate the role and performance of the cyber function

With all the cyber technological advances occurring every day, a CISO's No. 1 vulnerability continues to be attracting and retaining qualified people in the function.

While cyber executives increasingly manage seven-figure budgets, their rank and authority within the organization have not kept up with the speed of change. Many CISOs still report to a chief information officer or chief technology officer, and their budgets are often part of the IT budget. EY research found that for a majority of C-suite leaders (68%), cybersecurity is part of the IT budget. This puts cybersecurity in direct conflict with a multitude of operational business priorities rather than on footing with more strategic aspects of running the business, such as manufacturing operations, finance and business transformation.

As a CISO, it is critical to establish your role as a position of ownership over the organization's security posture and budget, with a mandate to drive strategic security. This may require you to negotiate with superiors, contend with conflicting priorities and navigate organizational politics.

> "The CISO position needs to be elevated to the level of all the other C-suite positions. Elevating the CISO will only help an organization with its security posture.
>
> Ayan Roy
> EY Americas Cybersecurity Competency Leader

Once you are comfortable with your position, it's important to quickly turn to your team. It's worthwhile to benchmark the size and scale of your cyber operating model and review audit and internal control findings to understand potential gaps. Then you can develop a plan for short-term improvements and more long-term considerations for next-generation cyber capabilities, including artificial intelligence (AI) and advanced analytics, as well as the skilled talent needed for an evolved function.

It's critical that you have a cyber leadership team ready to execute your vision. Don't be afraid to delegate; every hour you spend doing things that should be entrusted to other people is time you could be spending on higher-value matters. Meet with cyber leaders and teams across the company within your first 90 days. Be visible. Demonstrate genuine interest in what your team does. Take time to get to know people at all levels of the organization — and let them get to know you. Communicate often, showing your personal side as well as your business side. Embrace vulnerability by acknowledging that you don't have all the answers, while confidently expressing your commitment to safeguarding the company as it pursues its growth aspirations and strategic priorities.

It is also important to seek external perspectives to understand leading practices and the latest industry developments. Understand the various industry groups, training opportunities and conferences available, then consider whether participating in these forums will be accretive to the cyber strategy you seek to build. Proactively seeking external mentors and coaches from across your industry is another way to broaden your perspectives and further establish relationships that you may need to call upon later in your tenure as a CISO. These individuals can be extremely valuable as you navigate your personal career journey, either inside or outside your current organization.

When it comes to AI, CISOs are particularly optimistic about its ability to positively transform their organization's cybersecurity strategy and preparedness. Ninety percent of CISOs say AI is a critical component of their cybersecurity strategy.

Source: EY research.

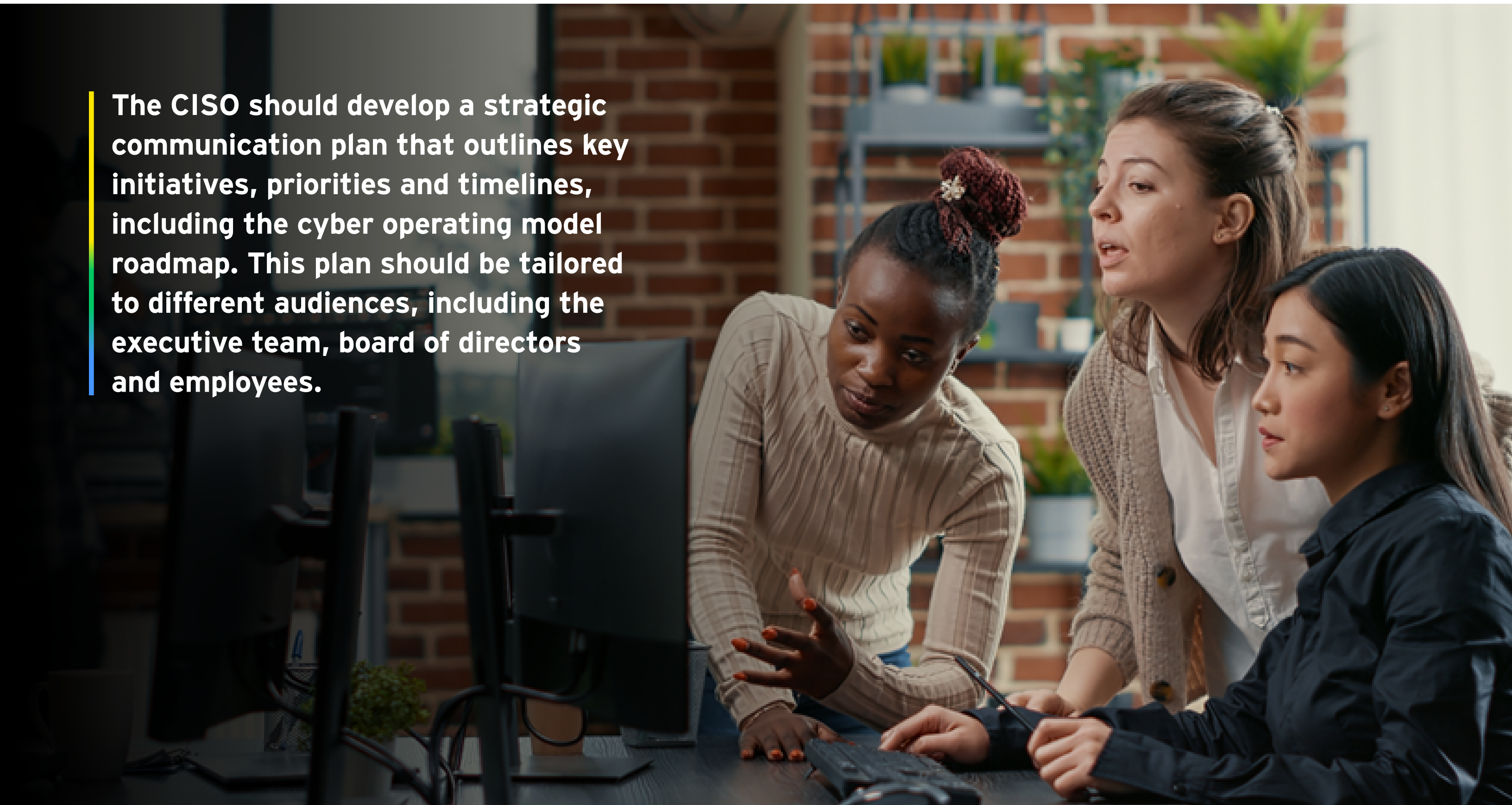
5 Communicate your vision and agenda

Based on everything you've learned, articulate your vision and communicate your agenda.

As a CISO, defining a clear vision for the cybersecurity program is essential for establishing credibility and direction within the organization. It is important that your vision aligns with the organization's overall business objectives, emphasizing the importance of cybersecurity in innovation, product development, protecting assets, facilitating compliance and fostering customer trust. This may also include the opportunity for embedding key security controls within existing processes and programs from the beginning to instill trust by design vs. the perception of security as an afterthought. This vision should be both aspirational and actionable, providing a roadmap for the future of the cybersecurity program. Early, well-planned changes send a strong message of intention while indicating where to expect changes and confirming your actions don't come across as too radical.

After defining the vision, effective communication of the agenda is crucial for gaining buy-in from stakeholders at all levels. Don't let the budget constrain you from asking for what you need. Go on the record with what will be required to protect the organization. Early on in your tenure, you have the luxury of being able to articulate gaps and ask for more — and with appropriate justification, you might just get it.

The CISO should develop a strategic communication plan that outlines key initiatives, priorities and timelines, including the cyber operating model roadmap previously described. This plan should be tailored to different audiences, including the executive team, board of directors and employees. Verify that each group understands its role in supporting the execution of the cybersecurity strategy. Regular updates, presentations and educational sessions can help keep stakeholders informed and engaged. By fostering an open dialogue and encouraging feedback, the CISO can create a culture of collaboration and shared responsibility for cybersecurity, ultimately enhancing the organization's resilience against emerging threats.



> **The CISO should develop a strategic communication plan that outlines key initiatives, priorities and timelines, including the cyber operating model roadmap. This plan should be tailored to different audiences, including the executive team, board of directors and employees.**

Your CISO checklist

1 Review your current state security posture across the organization

□ Assess policies, procedures, technologies and the incident response plan, then identify strengths and gaps.

□ Consider a third-party assessment to determine the current maturity level of the cyber function to help prioritize areas for investment.

□ Conduct a listening tour with the C-suite, business unit leaders and your cyber team to gather concerns and find quick wins.

□ Dig into the policy exceptions – what are the hidden risks?

□ Understand the current technology tool stack coverage and look for rationalization opportunities where potential overlaps and gaps may exist.

□ Review where your dollars are being spent today – which vendors, licenses, etc.

□ Develop a strategic roadmap to outline improvements and achieve the desired future state of the cyber function.

2 Build trusted relationships with key stakeholders

□ Quickly demonstrate your grasp on the business: value drivers, performance, strategies and priorities.

□ Meet with all C-level business unit and functional leaders to understand their candid perceptions of cyber.

□ Build a trusted relationship with the chair of the board committee tasked with oversight of cybersecurity and leverage this relationship for guidance on how to best interact with the full board of directors.

□ Map agendas of other executives against your cyber priorities to identify supporters and blockers.

3 Enhance culture and awareness

□ Develop and implement an engaging and tailored training program (using a mix of formats to accommodate various learning styles) across all three lines of defense that addresses the specific needs of different roles within the organization in managing and mitigating cyber risks.

□ Consistently communicate the importance of cybersecurity through various channels, including newsletters, town hall meetings and internal communications.

□ Foster an open culture where discussion about cybersecurity is encouraged and employees feel comfortable discussing security concerns.

□ Implement a straightforward process for employees to report suspicious activities or potential threats; ensure employees understand that there will be no repercussions for reporting.

□ Recognize and reward individuals or teams that demonstrate exemplary security practices.

□ Incorporate cybersecurity into the organization's core values and mission, confirming that all employees understand that cybersecurity is a shared responsibility, not just the domain of the IT or security teams.

4 Elevate the role and performance of the cyber function

□ Understand the cyber operating model and benchmark its maturity and capabilities. Set aspirations and a plan to elevate your cyber function.

□ Meet with all key cyber leaders and teams across the company within your first 90 days and assess whether your leadership team will be ready to execute your vision and the changes you define.

□ Question the usefulness of information in the cyber board reporting packages and determine what needs to change.

□ Review audit and internal control findings to understand gaps in processes and performance.

□ Ensure you and your team leverage industry groups, peer networks, external courses/trainings and cyber conferences/forums to stay current on industry trends.

□ Consider the implications of AI and machine learning in managing risks and in fulfilling the tasks of the function.

□ Engage with regulatory bodies and develop a technology-driven process to stay aware of changes in regulations and industry standards.

5 Communicate your vision and agenda

□ Go public with your vision and commitments; share them with the organization to instill confidence.

□ Take specific actions that both demonstrate near-term wins and that will enable the long-term security of the organization.

□ Crystallize the goals you are evaluated on and how your success is measured.

□ Understand your blind spots, form a plan to develop expertise and spend extra time outside your comfort zone.

□ Define your long-term career goals and create your personal development plan, which may include your personal aspirations as a CISO outside of the company.

□ Take advantage of internal and external leadership development opportunities and continue to grow your skill set; commit to continuous learning and remain intellectually curious.

□ Look for mentors, industry experts and leaders inside and outside of your company and join a CISO network.

Ernst & Young LLP contacts

Brian DePersiis

EY Americas Cybersecurity
Strategy Leader and CEL
CISO Program Leader

brian.depersiis@ey.com

Katie Karlix

CRO and CISO Programs Director

katie.karlix@ey.com

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multidisciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.

US SCORE no. 27927-251US_2
2507-10795-CS
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com