NIGHTDRAGON

SPECIAL REPORT: THE EVOLVING ROLE OF THE CHIEF INFORMATION SECURITY OFFICER

Top cybersecurity leaders in the NightDragon Advisor Council provide perspective on the changing role of CISOs and cyber leaders in 2024

Foreword

It seems today that no matter how quickly the cybersecurity landscape continues to advance, no enterprise is safe. And, regardless of how many digital bad actors are stealing sensitive data, crippling operations, and holding businesses hostage in hopes of a huge payday, the Chief Information Security Officer (CISO) continues to bear responsibility for securing their organization's environment.

As threats and technology continue to evolve, so does the role of a CISO. In a recent NightDragon survey of CISOs from some of the world's largest companies, nearly half of the respondents said the scope of their role evolved significantly within the last year alone. With these new responsibilities including taking on new duties, new accountabilities within the company, and new organizational functions, it's hard to imagine a slowdown for CISOs any time in the near future.

This is a significant statement regarding a role that is already expected to often operate 24/7 and where a single misstep or incident can leave a security leader looking for a job or, worse, under federal investigation.

While most CISOs reported feeling supported by their CEO and board of directors, there is still work to do to address challenges like talent shortages, budget availability, and management of limitations that make the CISO's job harder. AI is also changing the role of CISO, according to 48% of respondents, as is increased investment in new technology, like the cloud and risk quantification.

This is why it is critical for organizations to support CISOs, whether it's ensuring they have clear roles, responsibilities, support, or the resources they need. When CISOs have a voice, it changes the company's entire approach to defending its IT environments. Enterprises can shift to a more proactive approach to addressing vulnerabilities and exert tighter control over their IT environments. This is especially important as AI drives new defensive, detection and recovery capabilities. While hackers will never stop, enterprises can get much better at protecting, detecting and recovering from an attack.

In this report, we'll dig deeper into the evolving scope of the CISO, the roadblocks that many still face in trying to execute, and the opportunities ahead as AI transforms the cybersecurity landscape. Our hope is to both educate leaders and organizations on how they can help support their CISOs, and more importantly, arm existing and future CISOs with the knowledge and skills needed to mitigate today's threats. The struggles exist, but so too do the opportunities.

Dave DeWalt
Founder and CEO, NightDragon

Table of Contents

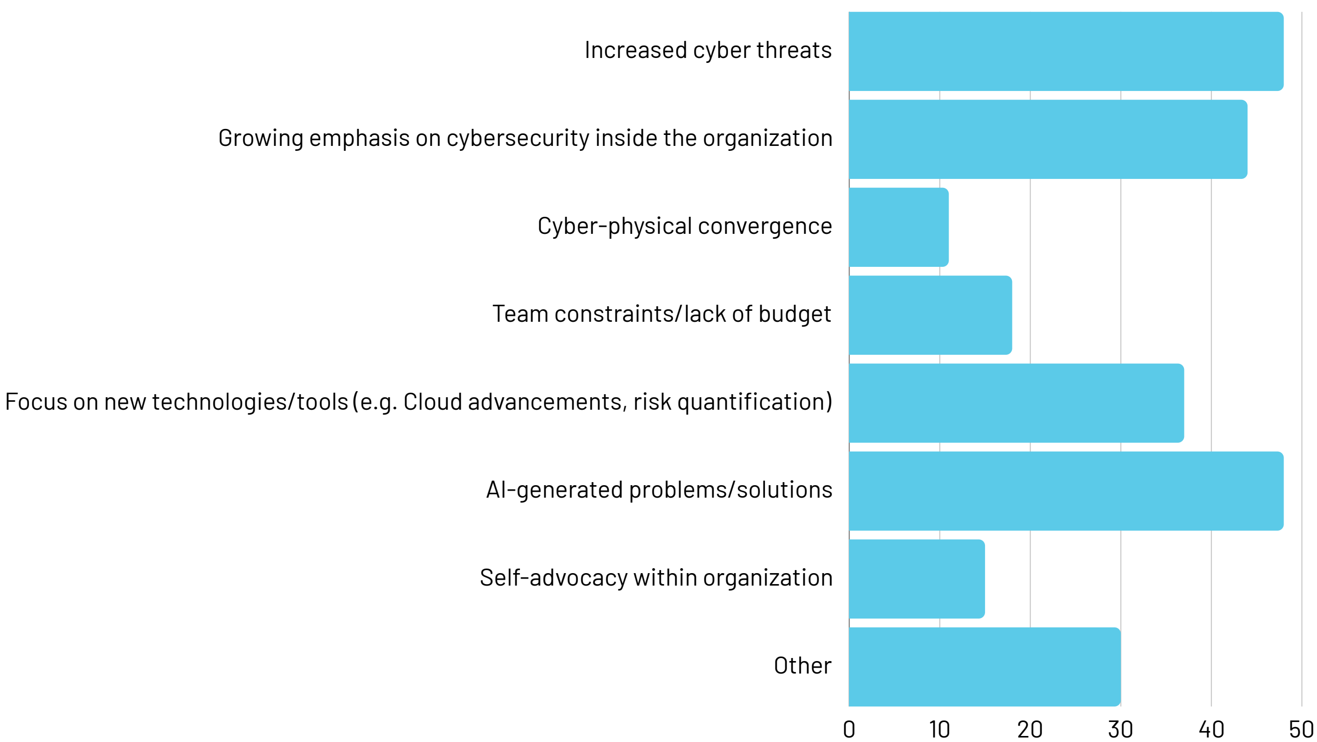
Introduction

In this survey, we polled NightDragon's Advisor Council – inclusive of 100+ Fortune 500 CISOs and cyber experts with experiences ranging from enterprise to public sector and healthcare to finance to critical infrastructure. While the findings were generally positive, the data suggest ample room for improvement.

Findings

Few roles have seen their jobs shift as much as Chief Information Security Officers. Approximately half of CISOs surveyed said their role has changed "significantly" over the past year.

What's driving that change? CISOs shared:



In a focus group discussion, CISOs shared areas that they are experiencing additional responsibility for, including:

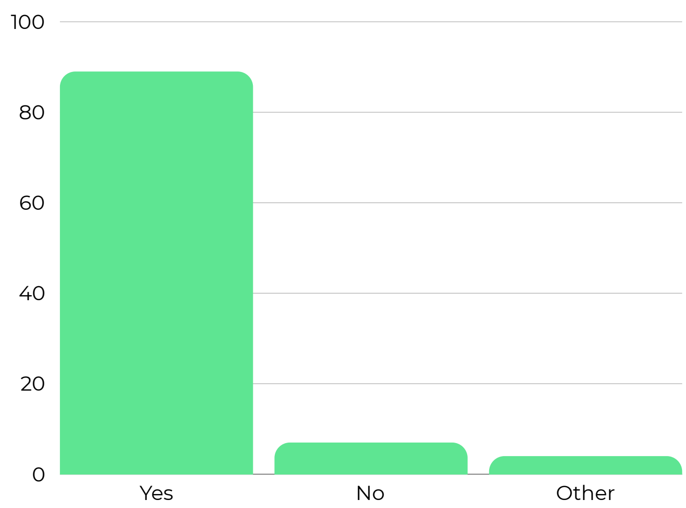
- Infrastructure
- Risk
- Fraud
- Physical Security
- Artificial Intelligence

"I'm seeing the role evolve to include more technical functions beyond the typical CISO area of responsibility, including blending infrastructure with more traditional IT functions alongside the cybersecurity function,"
- ASHLEY DEVOTO, CISO, Discount Tire

"The evolution of the CISO includes taking on additional functions, such as: operational resiliency, due diligence, AI implementation, privacy/legal considerations and regulatory compliance,"
- MIKE ROSEN, CISO, ZwillGen

While this additional responsibility is seemingly accompanied by leadership support, many CISOs also stated an ongoing lack of clarity into expectations and responsibilities for the role. Knowing the exact parameters for which a CISO is responsible is not always well-defined. In the words of one CISO, "sometimes it feels like we're defined as the Chief 'Look around the Corner' Officer," responsible for any mix of security, business, or any number of technical issues that arise.

Do you feel supported by your CEO and/or Board of Directors in your role as a cyber leader?



This can cause a lot of stress for CISOs if they are not in control of what areas they are increasingly responsible for, said Katie Jenkins, CISO at Liberty Mutual. “Role expansion is optimal when it comes through the intentional advocacy from the CISO of the additional functions that support operational efficiency and mission. In contrast, role expansion can be a stressor when done in a way that is not complementary to needs and interests of the security organization, and merely added with an ill-defined purpose or mandate,” she said.

“There is still not a clear job definition, so the lack of clarity in the role creates a lot of stress. Often, the CISO becomes the general problem solver– even if it’s not a cybersecurity problem! I've found that it falls to us because CISOs are both team players and problems solvers,” said George Eapen, CIO at Petrofac.

Setting clear priorities, either upon taking a role or throughout the process of your tenure, can help mitigate some of this ambiguity, CISOs said. “There aren’t infinite amounts of budget, and you can’t accomplish 80 things in one year, so prioritization is supremely important,” said Dave Baumgartner, Former EVP, Mandiant, noting that the CISO can play a strong role in setting that agenda alongside management. “You have to be willing to reach out and grab areas of adjacencies that are important to you and bring that business component into the role.”

Current CISO Pain Points

CISOs provided perspective on what areas they struggle the most with within their roles. Here’s what they had to say:

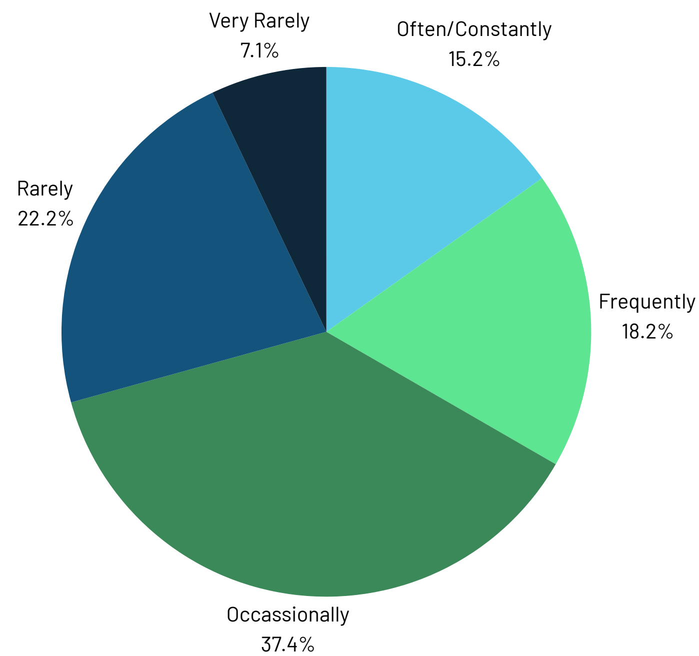
- Budget considerations
- Access to talent
- Prioritization of risk in the business
- Limitations of management/company culture
- New threats
- Measurement and reporting

Spotlight on Mental Health

CISOs have arguably one of the most stressful jobs in the C-suite. The team must be alert around the clock or run the risk of compromise or even entire shutdown of the organization. To add even more pressure, there's the looming threat that, in the event of an attack, the CISO can be held liable and lose their job or even face jail time.

The result? A significant impact on the mental health of security teams and their CISO leaders. 70% of CISOs surveyed said the job negatively impacted their mental health. CISOs described an unrelenting and often thankless job, where demands for budget and resources are not always met as they look to fight an ever-changing threat landscape.

How often has your role as CISO negatively impacted your mental health beyond just common executive pressure?



"We're all under stress to meet the demand of the evolving threat landscape... It's leading to a lot of burnout and turnover," said Tim Roemer, Chief Security Officer for GMI.

"You can have all the resources in the world, but still be exposed by a very good adversary. Be mentally prepared because your best day can quickly be turned into your worst day over and over again... It's not an easy job, and you have to psychologically be okay with that," said Dave Baumgartner, Former EVP, Mandiant.

One area that many CISOs said helped them feel more supportive was through the building of community to commiserate over shared challenges or experienced, brainstorm solutions and more. Examples could include CISO meetups, 1-1 conversations with peers, joining Advisory boards, and more. "You're not alone!" said Neil Boland, CISO for MLB.

Spotlight on Mental Health

Supporting Security Teams with Mental Health

While CISOs have a challenging job, their teams face many of the same stressors and pressures. With that in mind, mental health is extremely important for CISOs to prioritize with their teams to support employee happiness and ensure retention, said Barbara Massa, Partner at NightDragon and former Chief People Officer at Mandiant.

Here are some ways that CISOs can support their teams:

- Check In - CISOs and managers should check in on employees regularly on how they are feeling, as well as if there are new areas they'd like to learn to feel fulfilled. Barbara called this a "stay interview," rather than waiting for an exit interview to find these things out.
- Recognition - Take time to recognize those employees who do outstanding work for the organization. This could take the form of public recognition in a team meeting, a thank you in a 1-1 or other format that is best suited for the employee's personality and preferences.
- Expand Your Skills - While security team members have a lot of tasks on their plate, it is also important to take time to learn new skills and break out of the day-to-day pressure. Check in with employees to see what skills are interesting to them and set up time for them to shadow other employees or pursue education.
- Provide Access to Resources - Mental health is critical and a CISO can exemplify its importance by providing access to resources to support employee's mental health, including meditation apps or online therapy resources.
- Measure Engagement - Effectiveness of these efforts can be measured in a number of ways, including regular pulse surveys, the number of people taking advantage of the programs, and attrition data.

Barbara Massa
Partner, Chief Operating Officer, NightDragon

Evolution of the CISO Team

According to the World Economic Forum, 52% of public organizations said a lack of resources and skills is their biggest challenge when designing for cyber resilience. This gap becomes even more pronounced as the CISO role evolves. The ongoing integration of AI into cybersecurity roles has further accelerated the talent gap, as cyber leaders strive to maintain or recruit professionals competent in the relevant skills to address this new technology category. A CISO once ready to face its organization's needs may no longer feel equipped as new technology emerges.

Below are some tactics CISOs cited to address some of the new aspects that have become inherent to their role.

- Review the expertise of your team: Leaders should take an inventory of the skills and capabilities of their team, especially as it pertains to new areas like AI. This will give you an understanding of where your current team sits by way of expertise.
- Identify areas of growth: Once you have an inventory of the skills available, you now have a roadmap for if they need to either recruit new talent, or train and upskill the capabilities of current team members to tackle your biggest challenges and make an impact on the risk profile of the organization. New hires should be mapped against these high-priority areas, whether it is AI or cybersecurity skills.
- Cultivate experts: In areas where it can be difficult to find talent, some CISOs said they train their own. While this can take longer, they said those employees trained from the ground up tend to have fewer retention challenges than those hired more traditionally.
- Bring Board awareness to the issue: The CISO can be the biggest advocate to the Board and other leadership for what the team needs to succeed, as well as help key stakeholders understand the risks and threats the organization faces.

Just as the CISO role evolves to meet new threats, so too should the security team. By constantly evaluating the expertise, identifying areas of growth and advocating within the organization, a CISO can help stay nimble and prepare the organization for today's threats and opportunities, as well as those that may come in the future.

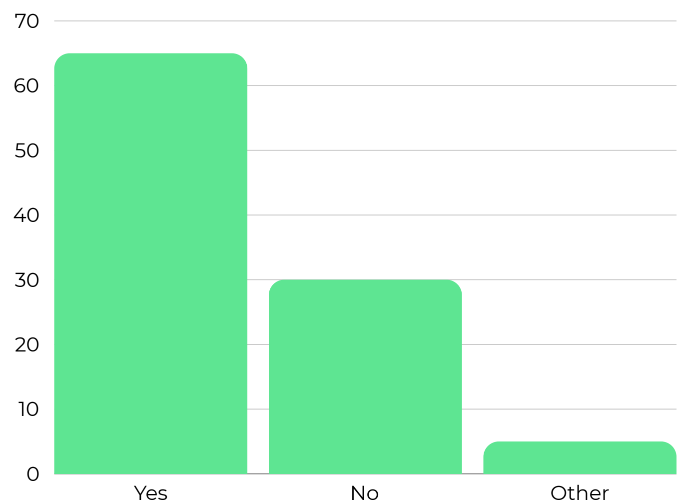
Effective Business Leadership

The majority - 65% - of CISOs told us they expect more of a leadership role in the coming year. This requires CISOs to learn the language of business, speaking to both technical teams and non-technical business leaders about the company's cybersecurity tactics and strategy. It also necessitates thinking less about only day-to-day defensive operations and instead focusing also on making cybersecurity a more fundamental part of how the company runs.

"This is, in many ways, a golden time to be a CISO... However, this combination of skills is unlike anything the market has seen. To be the most impactful CISO for the organization, you will need to help create a common language that deciphers risks when addressing the people, process, and technology," said Michael Piacente, Managing Partner at Hitch Partners.

George Eapen, CIO at Petrofac, agreed, saying, "Management doesn't care about breaches or incidents. They are worried about impact," he said. "The CISO role is now a business role and less of a technical one."

I expect to see an increasing leadership role for myself within the organization within the next year.



So what must a CISO keep in their toolkit? One skill is clear communication. A CISO must effectively communicate complex security concepts to a diverse range of stakeholders, including board members, employees, and external partners. This will help the CISO get buy-in across the organization for their strategies and help these stakeholders understand the risk the business faces. Emotional intelligence is also crucial in connecting across the organization and overcoming employees' resistance towards security measures.

"Soft skills like effective communication, influencing others, and mentoring people are important. Most of these skills I learned from emulating effective leaders around me and from making mistakes and learning from them," said Brad Schaufenbuel, CISO, Paychex.

Conclusion

The role of the CISO has never been more important as cyber damages continue to rise into the trillions of dollars, and even in some cases put lives at risk. As our survey found, while important, it can also be a difficult, grueling job that requires a unique combination of technical skills, leadership acumen and personal attributes. We also must do better as an industry to ensure we are all educated, from the individual contributor up to the board director, on cybersecurity, and we are enabling CISOs with the resources and talent needed to build a more secure future.

As technology advances and cyber threats evolve, it is important for all of us to stand alongside CISOs and help support their important mission.

Afterword

At NightDragon, we thank all the valuable and talented members of our NightDragon Advisory Council for their contribution to this report and the vital role in securing our world for tomorrow, as well as every other CISO across the industry.

The road ahead for CISOs will not be easy as their skills become increasingly important in the digital age and the threats grow. We owe these leaders a great debt for their service to secure organizations and our nation. Better collaboration, increased support, and dedicated advancement of technology and skills will help their organizations perform more effectively and efficiently as they fight back against the threats of today and tomorrow.

Thank you NightDragon Advisors and to the broader CISO community for your contributions to this work.

The NightDragon Team

Media Contact

NightDragon
Sarah Kuranda Vallone, VP Marketing
sarah@nightdragon.com