Deloitte.
University Press

New perspectives on how cyber risk can power performance

Cyber

Risk powers performance.

Sam Balaji
Business Leader
Global Risk Advisory

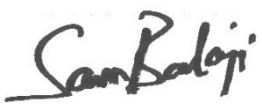
The traditional view of risk management solely as a means of risk avoidance is changing. Perhaps, it's time to raise the possibility that risk is something we not only *should* accept, but embrace. This includes cyber risk. Reports of cyber breaches and attacks surface with alarming regularity. These reports tend to focus on the negative impacts of cyber risk: the data stolen, the value lost, and the damage done. This is understandable. Bad news makes good press. But shouldn't we acknowledge that cyber risk is an unavoidable part of doing business today? And shouldn't we expand our view of this risk to include opportunity?

The answer springs from the notion that risk powers performance. There is no reward without risk—and this, in a world where digital technology is vital to all aspects of business, is especially true of cyber risk.

Business leaders understand that doing what needs to be done to create enterprise value often means taking risks. Think about the range of initiatives that today's organizations undertake to pursue innovation, accelerate performance, and enable growth: Using social media tools to attract customers and to change how employees collaborate and engage. Outsourcing non-core activities to an array of often-distant suppliers and vendors. Applying exponential technologies like the Cloud and the Internet of Things to transform the business. All of these actions rely on communication and data management through digital technology. In fact, there's no escaping the reality that virtually everything an organization does, in this day and age, relies on digital technology—and thus is accompanied by at least some degree of cyber risk.

As with all risk, cyber risk must be managed with an eye to the organization's risk appetite. But when managed from the perspective that risk powers performance, cyber risk begins to take on a different flavor. Far from always being undesirable, it emerges as a thing to be consciously taken, an inevitable concomitant of growth. Leadership's task is to enter into situations that entail cyber risk with their eyes wide open so that understanding the risk, they can take steps to address it.

I encourage you to read the articles in this collection and use them to further conversations in your own organization about leveraging cyber risk to power performance.



Sam Balaji
Business Leader
Global Risk Advisory


CISO

The new CISO

Leading the strategic security organization

By Taryn Aguas, Khalid Kark, and Monique François

Monitoring, repelling, and responding to cyberthreats while meeting compliance requirements are well-established duties of chief information security officers (CISOs), or their equivalents, and their teams. But the business landscape is rapidly evolving. An often-cited statistic holds that "90 percent of the world's data was generated over the last two years."[1] This explosion of connectivity provides companies new opportunities for customer growth and product development—but these opportunities come with a catch: As customer data, intellectual property, and brand equity evolve, they become new targets for information theft, directly impacting shareholder value and business performance. In response, business leaders need CISOs to take a stronger and more strategic leadership role. Inherent to this new role is the imperative to move beyond the role of compliance monitors and enforcers to integrate better with the business, manage information risks more strategically, and work toward a culture of shared cyber risk ownership across the enterprise.

Paradoxically, though CEOs and other C-suite executives may very well like the CISO's role expanded, these same executives may unknowingly impede organizational progress. While senior executives may claim to understand the need for cybersecurity, their support for the information security organization, and sometimes specific cybersecurity measures, can be hard to come by. For instance, 70 percent of executives are confident about their current security solutions, even though only 50 percent of information technology (IT) professionals share this sentiment.[2] So what's creating this organizational disconnect?

CISOs recognize they can benefit from new skills, greater focus on strategy, and greater executive interaction, but many are spinning their wheels in their attempts to get these initiatives rolling. Through insights uncovered from Deloitte's[3] CISO Lab sessions[4] and secondary research, we explore what barriers CISOs most commonly face when building a more proactive and business-aligned security organization, and describe steps they can take to become strategic contributors to the organization.

RECOGNIZE THE WARNING SIGNS

If executives and IT professionals have conflicting views on the necessity to expand the CISO's organizational reach, it may be critical to assess the warning signs. The need to elevate the CISO's role within an organization can manifest in several ways:

Leadership and resource shortcomings. The security organization's leader may be a business or IT director who lacks formal security training, is perceived to be tactical and operational in approach, or spends most of his or her time on compliance activities rather than cyber risk management. The function may have a small budget in comparison to the industry, with limited resources and skill sets, or the security program may not be adequately defined and may lack established processes and controls.

A security breach. An actual breach where data or systems are compromised can be a sign of systemic issues, operational failures, and, potentially, a culture that does not value security. Compliance lapses, audit issues, and a lack of metrics and transparency can all be harbingers of potential security problems as well.

Inadequate alignment with the business. Business units may view security as a policeman rather than as a partner. CISOs and their teams that do not make an effort to understand and partner with the business leaders often become roadblocks to the business achieving its objectives, which leads to employees circumventing the security team and security measures.

Organizational structural issues. The security organizational structure may not be well defined or buried several layers down in IT. A recent survey conducted by Georgia Institute of Technology sheds light on this issue: Only

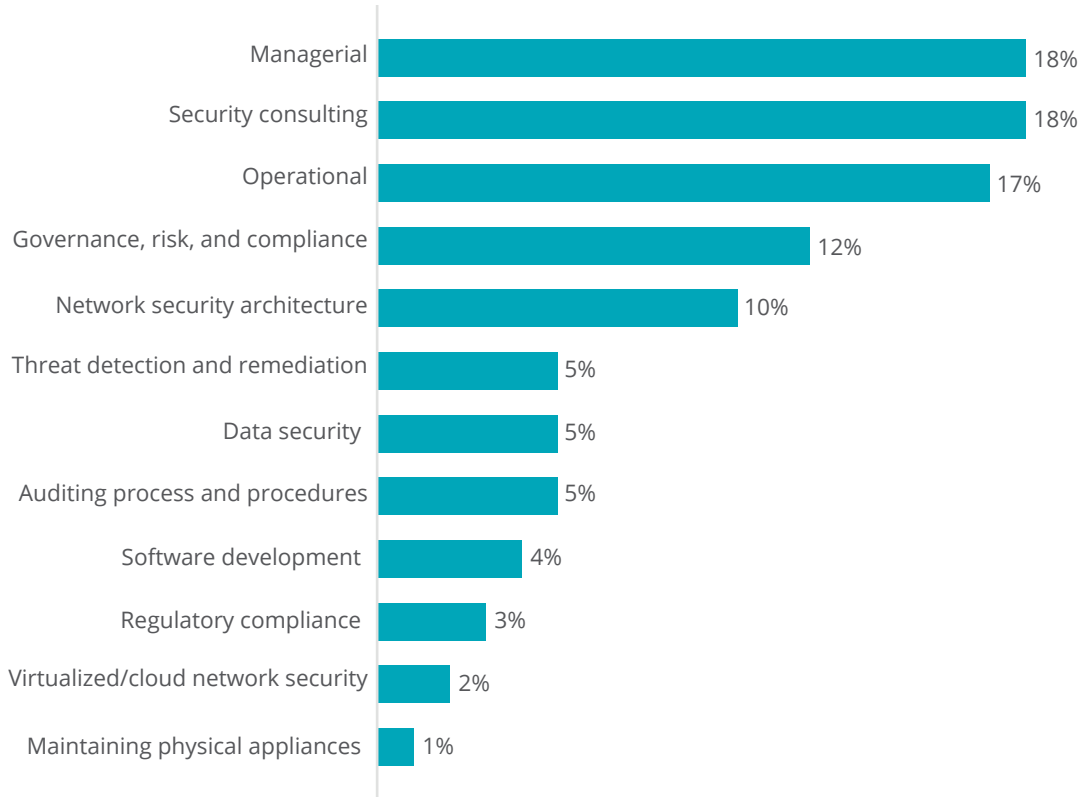
22 percent of respondents work in an organization where the CISO reports directly to the CEO, while 40 percent still report to the CIO.[5] And, whether housed in IT, risk management, legal, or operations, the security organization can be isolated from other areas of the business, impeding understanding and awareness of—as well as integration with—different functions.

Any of these signs can point toward a growing problem within an organization—one that simmers until a breach or other cybersecurity breakdown occurs, and the organization goes into crisis mode. This raises the question: Why isn't more progress being made?

CHALLENGES IN CREATING THE STRATEGIC SECURITY ORGANIZATION

WHY do companies struggle to strengthen cybersecurity? What factors are keeping CISOs from taking a more strategic enterprise role? The causes can lie within the security organization, in business units, and in communication between the two.

Figure 1. CISOs' former professional roles



Note: This figure shows the roles CISOs previously held before moving into the security organization.

Source: Frank Dickson and Michael Suby, *The 2015 (ISC)² global information security workforce study*, Frost & Sullivan, 2015, p. 36.

Graphic: Deloitte University Press | dupress.deloitte.com

Looking inward: When the CISO needs to look in the mirror

According to data from Deloitte's CISO Labs, building capabilities to better integrate with the business is a consistent priority among CISOs. Over 90 percent of CISOs hope to improve the strategic alignment between the security organization and the business, yet nearly half (46 percent) fear the inability to accomplish that alignment.[6] Why is that?

Narrow perspective. Because most are technologists by training and trade, CISOs typically have had limited exposure to and knowledge of the overall business. Before rising to management positions, many CISOs hold roles ranging from maintaining physical appliances and developing software, to compliance-related activities, threat detection/remediation, and network security architecture (figure 1).[7] If they don't receive management training that includes business and business development skills, this narrow perspective can impede CISOs' ability to view cyberthreats not simply as technical requirements but as critical risk issues—the latter a perspective vital to becoming a strategic player across the enterprise.

Communications and collaboration. CISOs can also struggle to communicate and collaborate with business leaders, in part because of limited interactions and relationships with them, a problem exacerbated by perceptions at the executive level. Most of Deloitte's CISO Labs participants (79 percent) reported they were "spending time with business leaders who think cyber risk is a technical problem or a compliance exercise." As a result, most CISOs "have to invest a lot of time to get buy-in and support for security initiatives."[8]

Those relationships are essential, though, in understanding what's happening in the business and where the greatest risks lie. For example, since it is virtually impossible to protect every piece of data in an organization, a security leader needs to work with the business to understand which data is critical to the enterprise, where it resides, and the impact should it be lost or compromised. Such exploration can suffer from a lack of clearly defined communication channels. Security doesn't have the tight integration and back and forth with the business enjoyed by functions such as customer service (which regularly provides information on customer demands and trends to other key functions) or finance (which delivers dollars-and-cents data to stakeholders across the organization).

Talent shortage. The lack of security talent can also keep the CISO from focusing on big-picture issues. The No. 1 reason CISOs stay mired in the weeds is because they have too few team members and not enough experienced talent.[9] Security is still a new skill set, one that is highly specialized and in high demand. According to a 2015 Frost & Sullivan survey, 62 percent of respondents said their organizations lack a sufficient number of security professionals, up from 56 percent just two years earlier. Furthermore, Frost & Sullivan predicts

"It's challenging to find people with the right skills, but the bigger problem is that it's a 'buyer's market.' Cyber professionals at almost every level have many options in front of them when deciding where to work. To be successful in attracting them, we have to make sure we convey the quality of our culture and the value of the contribution they can make."

—Genady Vishnevetsky, CISO, Stewart Title

that there will be a shortage of 1.5 million security professionals by 2020.[10]

Looking outward: The organizational climb of the CISO

Beyond issues specific to the CISO and team, security leaders also face headwinds from the broader business. Business program leaders often do not see the value of investing time and resources in understanding security beyond its more traditional functions. In contrast, they may be comfortably involved in other technology areas, such as the implementation of a customer relationship management (CRM) system, because they readily grasp the underlying business issues. Our research indicates two primary reasons for the lack of cyber risk focus at the organizational level: a false sense of security and competing agendas.

False sense of security. Many business-unit and C-suite executives think compliance equals security, especially in highly regulated industries. In Deloitte CISO Labs, 79 percent of CISOs report spending time with business leaders who think cyber risk is a technical problem or a compliance exercise.[11] However, being compliant with regulations does not address all cyber risk or make an organization secure, and that mind-set can create an organizational culture that has a very narrow and inadequate understanding of cyber risk.

Competing agendas. Business leaders have a role to play in elevating the importance of enterprise security, but it is a role many may view indifferently at best. A recent ThreatTrack survey revealed that 74 percent of C-suite executives do not think CISOs should have a seat at the table or be part of their organization's leadership team.[12] One reason may be that the mission of business units is to create new products and services, drive sales and revenue, and control costs in the process. Their results are not typically measured by, nor are they held accountable for, security considerations, and they don't readily make the connection between their strategic growth agenda and the cyber risks they tend to create.

STEPS TOWARD THE STRATEGIC SECURITY ORGANIZATION

CREATING a security organization that is a more strategic, integrated partner of the business requires both a new view of the CISO's role and a concerted effort to create a culture of shared ownership for cyber risk.

Elevating the CISO role

Increasing the value that the cyber risk program delivers to the enterprise requires a balanced approach. A successful CISO determines early on how to balance priorities and challenges across "four faces" of the CISO: *technologist*, *guardian*, *advisor*, and *strategist* (see the sidebar "The four faces of the CISO").[13] While all four roles are important, CISOs are being challenged to move beyond a traditional focus on the technologist and guardian roles. If their day-to-day actions and activities lean toward strategist and advisor, they are more likely to be viewed that way by other senior executives.

Assuming strategist and advisor traits

Today, much of a CISO's time and resources are spent managing and responding to threats. CISOs typically focus on activities such as overseeing and directing the implementation of security tools and technologies, identifying and blocking the leakage of digital assets, and managing the risk of and response to cyber incidents. The difficulty in differentiating between what is more and less important can lead to lumping security risks together and trying to protect the whole environment.

Moreover, a CISO's understanding of and appetite for risk may be quite different than that of a business unit leader. While the CISO may think in terms of reducing risks, business leaders take risks every day, whether introducing an existing product to a new market, taking on an external partner to pursue a new line of business, or engaging in a merger or acquisition. In fact, the ability to accept more risk can increase business opportunities, while ruling it out may lead to their loss. From this perspective, the role of the CISO becomes one of helping leadership and employees be aware of and understand cyber risks, and equipping them to make decisions based on that understanding. In some cases, the organization's innovation agenda may necessitate a more lenient view of security controls. Enabling business agility may require the CISO to lead more finely tuned efforts to detect threats early, and to emphasize preparedness for possible cyberattacks. (See "From security monitoring to cyber risk monitoring" in this issue for a more detailed discussion about how organizations can evolve toward a risk-focused threat monitoring program.)[14]

Change the conversation from security to risk (strategist role)

Taking on a more strategic role requires CISOs to pivot the conversation—both in terms of their mind-set as well as language—from

THE FOUR FACES OF THE CISO

CISOs continue to serve the vital functions of managing security technologies (technologist) and protecting enterprise assets (guardian). At the same time, they are increasingly expected to focus more on setting security strategy (strategist) and advising business leaders on security's importance (advisor). (See figure 2.)

Technologist. The CISO as technologist guides the design, development, and deployment of secure technical architectures, instilling security standards and implementing innovative countermeasures. Technologists carefully select and implement platforms that support changing threat detection and monitoring solutions, and integrate services delivered by external sources into a seamless framework. Technologists ensure that architecture designs are flexible and extendable to meet future security and business needs. They develop and maintain the security policies and standards that an organization should adhere to, working with the CIO to ensure that platforms meet these requirements.

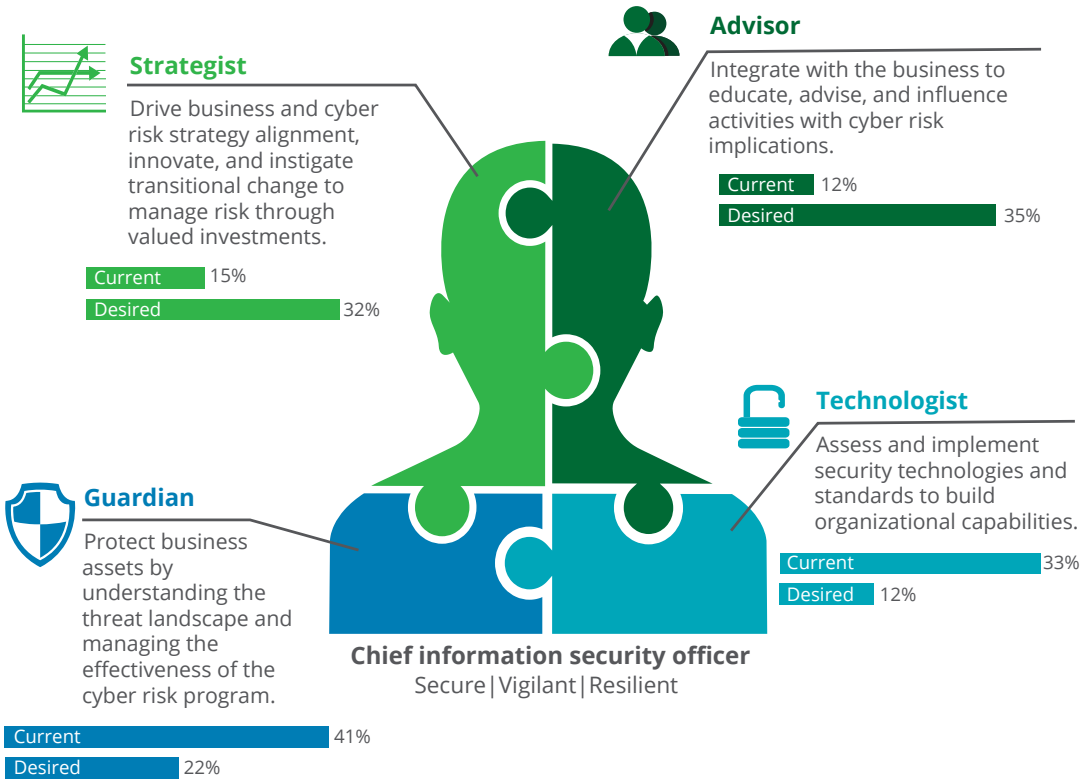
Guardian. As guardian, the CISO's charge is to monitor the effectiveness of the security program, processes, and controls in place. The guardian addresses considerations such as whether controls are working as intended, data is secure, and information is properly shared. Guardians monitor processes that safeguard the confidentiality, integrity, and availability of data and drive the overall security program. They also measure and report on information security risks to keep stakeholders informed and meet compliance and regulatory requirements.

Strategist. As strategist, the CISO is the chief value architect for all cyber risk investments. The strategist partners with the business to align business and information security strategies, and capture the value of security investments to safeguard enterprise assets. In this role, the CISO possesses deep business knowledge and acts as a credible partner who provides business-centric advice on how risk management can help the business. The strategist understands which business operations and information assets are the enterprise crown jewels, institutes strategic governance that prioritizes information security investments, and ensures that security and business resources and budgets are fully aligned to execute the priorities of the organization and deliver expected results.

Advisor. The CISO as advisor understands the implications of new or emerging threats, and helps identify cyber risks that arise as the business advances new strategies. The advisor drives the enterprise to continuously improve its security decision-making and risk mitigation capabilities. The advisor understands where the organization needs to focus to address cyberthreats, and creates a risk-based strategic roadmap to align cybersecurity efforts with corporate risk appetite. Advisors possess significant political capital and are able to enlist, educate, engage, and align executive stakeholders to increase security awareness.

security and compliance to focus more on risk strategy and management. Going beyond the negative aspect of how much damage or loss can result from risk, CISOs need to understand risk in terms of its potential to positively affect competitive advantage, business growth, and revenue expansion. For example, a CISO at a large retail organization used a three-tiered

Figure 2. The four faces of the CISO



Source: Research from Deloitte's CISO Transition Labs.

Graphic: Deloitte University Press | dupress.deloitte.com

risk model to present cyber risks to the board and discussed the mitigation plans for the most critical risks. He also updated the board on the risks business leaders decided to accept and why, including context on the business benefit.

Measure and report risk (strategist and advisor roles)

As the saying goes, what gets measured gets done. In cybersecurity, what gets measured gets noticed, so it is important for CISOs to define metrics that tell a story to which business leaders can relate. A CISO at a large technology company told a story about how he had run into his CEO in the hallway and told him that the team had blocked 125,000 malware attacks the previous month. The CEO's response was, "Isn't that your job?" The CISO acknowledged that he had blurted out the number without providing the right context.

To circumvent this issue, another CISO in a large financial services organization created a menu of security metrics, including acceptable upper and lower bounds for each metric, and then spent six months working with his

QUESTIONS TO SHAPE THE CYBER RISK ORGANIZATIONAL PROFILE

1. What are the key drivers of value in the organization, and how are these being protected?
2. What are the threats and vulnerabilities that provide the greatest exposure to us today?
3. To what extent do we have the foundational capabilities and practices in place to protect our critical assets?
4. How effective are we at monitoring and detecting cyber incidents?
5. Can we effectively respond to and recover from a cyber incident? Do we have response plans in place, and have they been tested?
6. What metrics demonstrate that we are effectively protecting the company?

stakeholders to create a custom cyber risk dashboard for each of their business areas. This helped the organization prioritize risk remediation as well as understand where risks may be acceptable.

In a report released by the World Economic Forum, cyber risk conversations should weigh three variables: the vulnerability of the system, the value of the assets at stake, and the sophistication of the attacker.[15] Bringing these three elements into the conversation highlights the relative importance of cyberthreats for business leaders. (To help facilitate these conversations, refer to the sidebar "Questions to shape the cyber risk organizational profile.") No longer is the conversation limited to issues of compliance; instead, business leaders can understand the costs of a threat that interrupts the business, as well as the likelihood of that event occurring in the current environment.

The CISOs who can align their risk metrics with the business's most pressing issues are more likely to be heard by strategic leadership. Making these insights easy to consume through intuitive dashboards can only help further solidify the CISOs' importance.

ADDRESSING TALENT DEMANDS

If CISOs hope to assume a more strategic role, they need to tackle organizational issues such as a shortage of security talent to support operational and technical activities—a key issue that can keep CISOs mired in minutiae. A recent Black Hat survey indicated that roughly 73 percent of organizations need more skilled security talent—a finding closely aligned with data from a Deloitte CISO Labs survey, which found that over 75 percent of participating CISOs noted a lack of skilled resources and effective team structure to support their priorities.[16]

To build upon organizational talent, CISOs should focus on developing a security-specific talent strategy that leverages existing skill sets, better integrates with stakeholders, and plans to fill the future talent pipeline.

Enhance the current workforce

The individuals you recruit or who are currently on your CISO team need to build their skill sets to accommodate the needs of the organization. One path organizations have taken is to cultivate relationships with technical institutes and universities to target specific skills needed, even establishing internship programs that focus on nurturing relationships with students and developing skills that align with the organization's goals and objectives. Another avenue of professional development comes from cyber risk "war games" training.[17] These are simulated scenarios designed to both test the readiness of an organization for specific cyber vulnerabilities as well as provide employees with hands-on experience for such events.

Integrate with the business

For fields outside of cybersecurity and risk, a number of studies have demonstrated that individuals with extensive "internal collaboration networks" routinely outperform those who work independently. These studies have been validated for fields such as engineering, research, and consulting.[18] In this spirit, it may be worthwhile for CISOs to focus on greater business collaboration that enhances the skill sets of both the cyber risk expert and the business leader.

The CISO may also consider developing an integration model by either designating cyber risk champions within business units or aligning cyber risk personnel with business units. Integrating talent resources can help employees understand where to go with security questions, and it can facilitate security professionals' understanding and awareness of business strategy and related cyber risk management requirements. The reality is that cybersecurity should be a priority for all employees. And, regardless of where the CISO function is positioned within the organization, it is important to understand where dotted-line relationships may exist and to clearly define roles to avoid confusion in responsibilities, and improve integration and collaboration.

Build future cyber risk leaders

In the longer term, it is important to consider both CISO succession planning and development of other leaders who can represent the CISO across the organization. Such candidates, manager level and up, need to be identified early and cross-trained, not just within security but across other areas of the business. Recently, George Washington University's School of Business has collaborated with the university's Center for Cyber and Homeland Security to offer a specialized "MBA with Cybersecurity" program to arm future organizational leaders with the "in-depth knowledge, resources, and network to drive global economics, innovation,

and policy" to meet the next generation of cyber challenges.[19] There are many other international programs with a similar focus, such as the MBA in Cybersecurity offered by Coventry University in the UK intended to enable graduates with the skills to "understand complex business problems and key issues in cyber security whilst exploring many associated business issues."

Such training can further build CISO candidates' credibility inside and outside the cyber risk function before they step into leadership roles, as well as help change the business perception that security professionals are purely technical and tactical.

LEADERSHIP EDUCATION, ENGAGEMENT, AND OWNERSHIP

HOW can CISOs secure executive support and involvement in encouraging cultural change and shared ownership of security across the enterprise?

Develop a communications strategy and plan

A CISO's communication plan should directly align with her or his vision and goals, and it should convey what success would look like for each functional area or executive role. Messaging should scale to all areas of the organization and be integrated with other business and functional messaging. Communications should highlight what is trending in security, both within the organization and in other similar businesses or government agencies. The discussion of those trends should be tailored so they are relevant to employees to help them understand the impact of the trend. Additional working tips and reminders about employee responsibility for keeping data safe can help drive the message home.

When communicating to the highest levels such as executive teams or boardrooms, make sure the messaging is on point and topical to the audience (see the sidebar "Communicating in the boardroom"). The plan should lay out how to establish conversations between leadership and the organization, whether through presentations, social media campaigns, or other means. This is an important step in setting the tone for broader culture change.

The goal is to clarify and justify a new view of risk and security, as well as inspire and catalyze employees to embrace it. One CISO hired two full-time media people on his team to spruce up his messaging and narrative to his leadership and to the rest of his organization.[20]

Enhance employee ownership by creating emotional connections

Studies from the fields of psychology, behavioral economics, and marketing have repeatedly shown that emotions rather than reason tend to drive human behavior. Because habits are tough to break with rational arguments alone, CISOs must inspire the business leaders who, in turn, must inspire employees to carry out the hard work of modifying their behavior and outlook.

COMMUNICATING IN THE BOARDROOM

Cyber risk is a business issue that board members may find especially challenging to oversee. In an effort to make the conversation more relevant and relatable, consider focusing your message on the following points:

- **Top cyber risks.** Tell the story of the current risk assessment results and the corresponding mitigation controls and management actions, particularly as they relate to top current business challenges.
- **Program maturity.** Explain your organization's maturity level in relation to the threat landscape and industry peers.
- **Emerging threats.** Identify who is attacking the company or its industry peers and the lessons learned. Explain news events and trends, such as the spread of ransomware or a high-profile data breach, and explain how they might impact your organization.
- **Audit and regulatory concerns.** Give status updates of any open audit and regulatory issues.
- **Public or private partnership.** Make note of any industry group participation and collaborations with law enforcement or intelligence agencies.

Many decisions the board wrestles with—whether related to new products, new markets, or mergers and acquisitions—are not directly about technology or security, but they have important cyber risk implications. A key objective for the CISO when interacting with the board is to become a trusted advisor who proactively helps illuminate these issues.

The Deloitte University Press article *Toeing the line: Improving security behavior in the information age* explains four behavioral elements that can modify organizational culture pertaining to risk practices:[21]

1. **Learning from policy.** Providing policies for employees to read is a natural first step. These are the artifacts that represent espoused values. However, policies alone will not sufficiently change behavior if the group does not act accordingly.

2. **Providing mentorship.** Social cues are a powerful influencer in determining what people value and how they should conform. Executives who embody new cybersecurity cultural attributes set a strong example for their direct reports and staff. When executives share their personal experiences in changing their own cybersecurity behaviors—and the challenges they've faced—they are more authentic, and their experiences can help other employees surmount similar hurdles.

3. **Group learning.** Draw from the work of consumer marketers in developing communications. For example, to foster more collaboration among employees, consider

having executives present examples of success stories from within the organization that highlight impactful cyber interventions at work.

4. **Learning from daily work.** Linking individual employees' day-to-day responsibilities to larger goals and to the organization's cyber resilience can give meaning to seemingly mundane activities. It can also lead to greater commitment and engagement. With more passionate employees, companies tend to derive greater productivity and profits.

These steps can help CISOs build credibility across the enterprise, fulfilling their role as advisor, and establish a work environment in which employees are empowered with security knowledge, requirements, and data to appropriately identify and mitigate risks on their own.

Table 1. Summary of CISO steps in the journey to a strategic security organization

Challenges	Steps to overcome them
Narrow perspectives	• Pivot the conversation from security to risk in order to facilitate more holistic conversations concerning the business • Stop viewing risk as categorically negative; calculated risks can lead to new business opportunities
Communication and collaboration	• Integrate with the business by developing cross-functional teams that include cyber risk specialists and business leaders • Borrow lessons from psychology and behavioral economics to create communications that speak to human behavior and thinking • Take advantage of a number of communication channels such as presentations, social media, and executive success stories
Talent shortage	• Explore partnerships with universities and professional organizations to enhance team skill sets • Leverage simulations and gaming scenarios to prep your team for high-risk events • Develop your "nontechnical" employees with leadership potential to be well versed in cyber risk
False sense of security	• Use dashboards to highlight current risk levels • Educate leadership on the difference between compliance and cyber risk management through communications and stories
Competing agendas	• Develop a stronger understanding of the business, and act as a strategist and advisor to the organization • Connect with leadership and the board to raise awareness; provide risk metrics that align with high-priority business efforts • Use communications and stories to create emotional connections that promote shared accountability

The importance of fostering an environment of security and risk awareness, shared ownership of cyber risk, and cyber risk resilience is only going to grow. CISOs who are able to step beyond a tactical, technical level are more likely to gain credibility and support among leaders across the enterprise, including the board, CxOs, and business unit leaders.

GAINING TRACTION, MOMENTUM, AND STRATEGIC DIRECTION

As cyber risks grow and evolve with technology advancement, so will the demands on CISOs, organization leaders, and employees. Instead of impeding innovation for fear of cyberthreats, the CISO should seek to be instrumental in aiding organizations to achieve their goals. The importance of fostering an environment of security and risk awareness, shared ownership of cyber risk, and cyber risk resilience is only going to grow. CISOs who are able to step beyond a tactical, technical level are more likely to gain credibility and support among leaders across the enterprise, including the board, CxOs, and business unit leaders. That is an important first step in leading efforts to create and sustain a culture of cyber risk awareness. Table 1 provides a summary of the other steps required to build a strategic security organization.

By earning a seat at the leadership table, helping imbue a shared sense of responsibility for cyber risk management, and providing guidance on how organizational leaders and employees can meet that responsibility, CISOs can become key drivers in the journey to the strategic security organization.

***Taryn Aguas**, a principal with Deloitte & Touche LLP, specializes in cybersecurity and technology risk management and leads Deloitte's CISO Lab program.*

***Khalid Kark** is a director with Deloitte Consulting LLP, where he leads the development of research and insights for the CIO Program.*

***Monique François** is a managing director with Deloitte Consulting LLP with over 20 years of experience guiding companies through complex change.*

Endnotes

1. "Big data, for better or worse: 90% of world's data generated over last two years," *Science Daily*, May 22, 2013, https://www.sciencedaily.com/releases/2013/05/130522085217.htm.

2. Barkly, *2016 cybersecurity confidence report*, http://cdn2.hubspot.net/hubfs/468115/Barkly_Cybersecurity_Confidence_Report.pdf, accessed April 11, 2016.

3. As used in this article, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

4. The Deloitte CISO Labs are immersive one-day workshops that encourage CISOs to think from a new perspective and develop a plan for success by focusing on the three most important resources a CISO has to manage: time, talent, and stakeholder relationships.

5. Jody R. Westby, *Governance of cybersecurity: 2015 report*, Georgia Tech Information Security Center, October 2, 2015, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/tech-briefs/governance-of-cybersecurity.pdf.

6. Deloitte CISO Labs data, 2015.

7. Frank Dickson and Michael Suby, *The 2015 (ISC)² global information security workforce study*, Frost & Sullivan, 2015, p. 3.

8. Deloitte CISO Labs data, 2015.

9. Ibid.

10. Dickson and Suby, *The 2015 (ISC)² global information security workforce study*, p. 36.

11. Deloitte CISO Labs data, 2015.

12. ThreatTrack Security Inc., *No respect: Chief information security officers misunderstood and underappreciated by their C-level peers*, June–July 2014, https://www.threattracksecurity.com/resources/white-papers/chief-information-security-officers-misunderstood.aspx.

13. Deloitte CISO Labs data, 2015. The "four faces of the CISO" concept is adapted from the framework presented in Ajit Kambil, *Navigating the four faces of a functional C-level executive*, Deloitte University Press, May 28, 2014, http://dupress.com/articles/crossing-chasm/.

14. Adnan Amjad, Mark Nicholson, Christopher Stevenson, and Andrew Douglas, "From security monitoring to cyber risk monitoring: Enabling business-aligned cybersecurity," *Deloitte Review* 19, July 2016, http://dupress.com/articles/future-of-cybersecurity-operations-management.

15. World Economic Forum in collaboration with Deloitte, *Partnering for cyber resilience: Towards the quantification of cyber threats*, January 2015, http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.

16. Black Hat, *2015: Time to rethink enterprise IT security,* July 2015, https://www.blackhat.com/docs/us-15/2015-Black-Hat-Attendee-Survey.pdf; Deloitte CISO Labs data, 2015.

17. Cat Zakrzewski, "Cybersecurity training, military style," *Wall Street Journal*, March 13, 2016, http://www.wsj.com/articles/cybersecurity-training-military-style-1457921566.

18. Jim Guszcza, Josh Bersin, and Jeff Schwartz, "HR for humans: How behavioral economics can shape the human-centered redesign of HR," *Deloitte Review* 18, Deloitte University Press, January 25, 2016, http://dupress.com/articles/behavioral-economics-evidence-based-hr-management/.

19. George Washington University, "World executive MBA with cybersecurity," http://business.gwu.edu/programs/executive-education/world-executive-mba/, accessed April 12, 2016.

20. Deloitte CISO Labs data, 2015.

21. Joe Mariani et al., *Toeing the line: Improving security behavior in the information age*, Deloitte University Press, January 28, 2016, http://dupress.com/articles/improving-security-behavior-in-information-age-behavioral-economics/.

TO LEARN MORE, PLEASE CONTACT:

Nick Galletto
Global Cyber Risk Services Leader
+1 416-601-6734
ngalletto@deloitte.ca

James Nunn-Price
Asia Pacific Cyber Risk Services Leader
+61 2-9322-7971
jamesnunnprice@deloitte.com.au

Ed Powers
US Cyber Risk Services Leader
+1 212-436-5599
epowers@deloitte.com

Chris Verdonck
EMEA Cyber Risk Services Leader
+32 2-800-24-20
cverdonck@deloitte.com

Ash Raghavan
Global Cyber Center of Excellence Leader
+1 212-436-2097
araghavan@deloitte.com

Deloitte has been widely recognized as a market leader, including these recent independent analyst reports:

- **Deloitte named a global leader in Security Operations Consulting by ALM Intelligence**
  Source: ALM Intelligence; Security Operations Center Consulting 2015; ALM Intelligence Consulting Research & Advisory estimates © 2016 ALM Media Properties, LLC. Reproduced under license
- **Deloitte ranked #1 globally in Information Security Consulting for 2015 based on revenue by Gartner**
  Source: Gartner, Market Share Analysis: Information Security Consulting, Worldwide, 2015, Jacqueline Heng, Elizabeth Kim, 05 July 2016