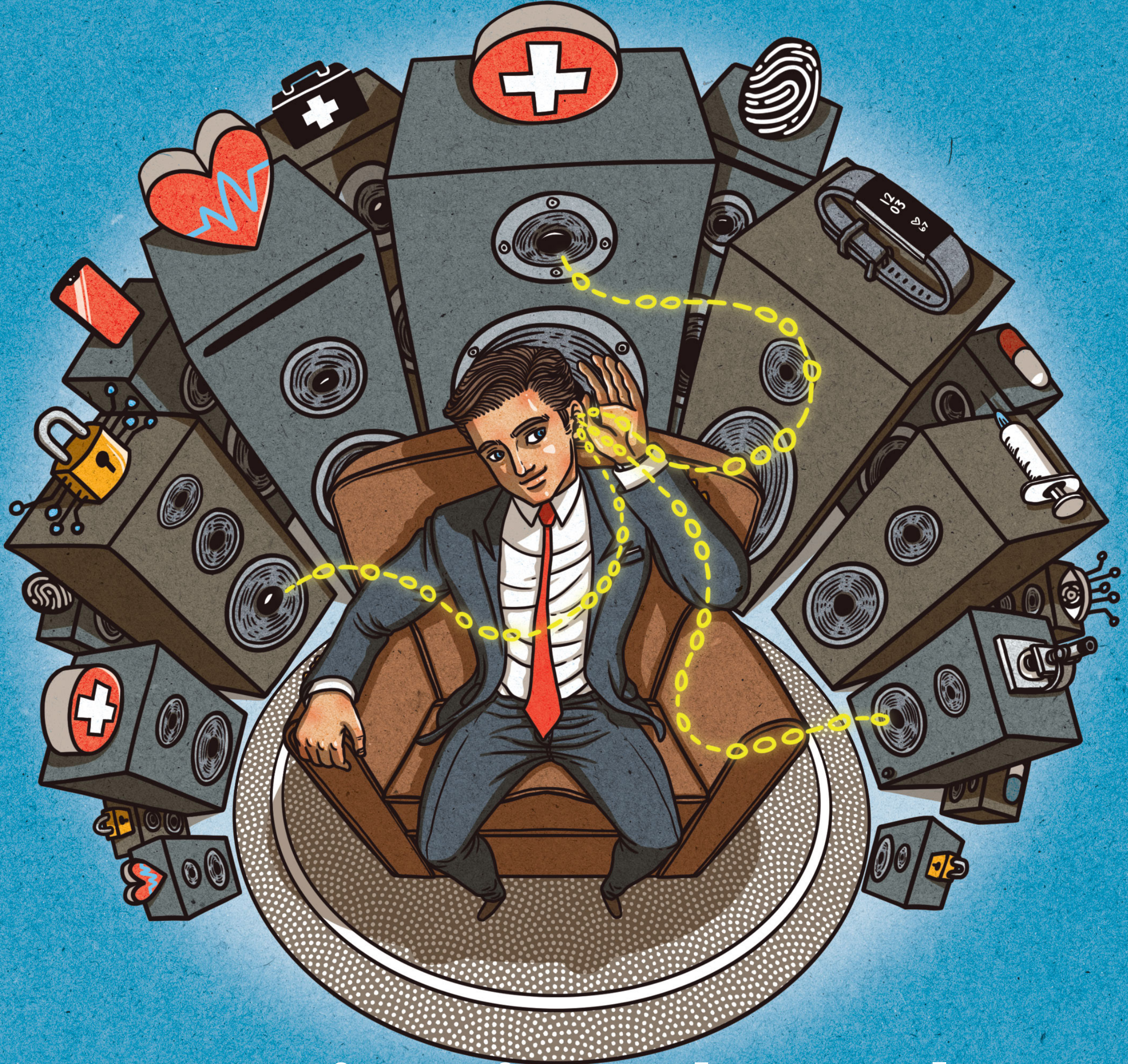
Deloitte.
Insights

A report by the Deloitte Center for Health Solutions



Communicating the value of cybersecurity to boards and leadership

Seven strategies for life sciences and health care organizations

Deloitte Risk and Financial Advisory helps organizations effectively navigate business risks and opportunities—from strategic, reputation, and financial risks to operational, cyber, and regulatory risks—to gain competitive advantage. We apply our experience in ongoing business operations and corporate life cycle. We leverage next-generation solutions in our Ventures Fund and Managed Services and Products business to help clients become stronger and more resilient. Our market-leading teams help clients embrace complexity to accelerate performance, disrupt through innovation, and lead in their industries. For more information on our Risk and Financial Advisory services, **visit www.deloitte.com/us/risk**.

Contents

Executive summary | 2

How well do board members and senior leaders understand cybersecurity risks? | 4

Seven effective strategies for communicating cybersecurity issues to the board and senior leaders | 5

Bringing a business perspective to cyber risk | 12

Endnotes | 14

Executive summary

THE VALUE OF cybersecurity should be crystal clear to life sciences and health care boards and leadership. Cybersecurity attacks and data breaches seem to be in the headlines almost daily, and sobering statistics are everywhere. The number of patient records impacted has nearly tripled in just one year, jumping from 5.5 million breached records in 2017 to about 15 million in 2018.[1] Health care data is valuable, and cybersecurity incidents can mean major costs for companies. Operations, for example, could be held hostage, the supply chain could be disrupted, legal fees could mount, and organizations could suffer meaningful but often difficult-to-quantify losses of reputation and consumer trust.

But communicating this risk to senior leaders and the board can be challenging, according to our research. "Cybersecurity is a top priority," one life sciences chief information security officer (CISO) told us. "But, there are many top priorities."

The board and senior leaders of life sciences and health care organizations are dealing with cost pressures and tightening margins, digital transformation, merger and acquisition activity, and fierce competition around consumer engagement. The role of the CISO is to support those broader concerns—" and do the best we can to minimize the risk and get the best value for the dollar." Cybersecurity communication is more than only communicating the bad things that might happen and explaining how the team is mitigating risks. The cybersecurity team also plays a key role in facilitating a seamless experience for consumers, and helping the organization make the best use of its data.

Board members (tasked with governance issues) or executives in senior leadership roles (tasked with operations) of life sciences and health care companies might not have a clear understanding of the interplay between cybersecurity and the business. Even though these leaders might rank cybersecurity as a top priority, when it comes to action, they might not fully understand and be able to act on the advice coming from CISOs and chief information officers (CIOs) in the best possible way.

To help identify leading practices for communicating the value of cybersecurity to boards and leadership, the Deloitte Center for Health Solutions interviewed 18 CISOs, CIOs, and C-suite executives from biopharma companies, medical device manufacturers, health plans, and health systems, who are involved in making decisions around cybersecurity. Our goal was to find out what is working and what challenges lie ahead.

We identified seven strategies organizations should consider to improve their communications around cybersecurity to their board and leadership (see figure 1).

CISOs and CIOs told us that a major goal underpinning their communication strategies is to help board members and senior leaders move to a "cyber everywhere" approach: an understanding that cybersecurity goes beyond the information technology bucket and can help reduce risk across the enterprise.

FIGURE 1

Seven strategies to improve cybersecurity communications to leadership

1 Create a dialogue to engage leadership and build trust

2 Use the power of storytelling to make it real

3 Help board members and leadership understand that a "cyber everywhere" mentality is the new norm

4 Explain how the cyber team is collaborating with people inside and outside of the industry

5 Use metrics to quantify risks, elevate the discussion in dollar terms, and connect it back to the business

6 Be prepared to answer and defend questions related to cybersecurity investments

7 Regularly assess and discuss future talent models and what they could mean for the organization

Source: Deloitte analysis.

Deloitte Insights | deloitte.com/insights

How well do board members and senior leaders understand cybersecurity risks?

PRIOR DELOITTE RESEARCH has shown that most people who serve on the board of public companies—as well as most members of senior leadership teams—do not have deep cyber-savvy or technology experience. Many executive boards are only beginning to add this kind of expertise. [2] The percentage of public companies that have appointed technology-focused board members has grown over the last six years from 10 percent to 17 percent.[3] There is also evidence that C-suite executives in many organizations lack the understanding and awareness needed to prioritize cybersecurity.[4] While the amount of technical expertise needed might be subjective, our interviewees said life sciences and health care organizations should strive to have a cyber-literate board and leadership to stay competitive. Regulators are also getting more serious about transparency in publicly traded companies. Moreover, in March 2019, a member of the House Intelligence Committee introduced a bill that would require public companies to tell investors whether any of its board members have cybersecurity expertise. The Cybersecurity Disclosure Act of 2019 is a companion bill to one introduced two years earlier in the Senate. The intent is to promote transparency in the oversight of cybersecurity risks in companies.[5]

Many interviewees said they focus much of their time communicating with board subcommittees, such as the audit committee or a technology committee. The goal in the coming months and years is to get the entire board to be more cyber-savvy. Only a small number of organizations said their entire boards were engaged on cybersecurity issues.

Given the challenges of the rapidly evolving ecosystem, how can CISOs and CIOs most effectively communicate the value of cybersecurity to board members and senior leaders? How can CISOs and CIOs connect the broader top-of-mind concerns, such as how to win the hearts and minds of consumers in a fiercely competitive landscape, with the more immediate issue of cybersecurity and enterprisewide risk management? Based on our interviews, and supported by research, we outlined seven targeted strategies.

How can CISOs and CIOs most effectively communicate the value of cybersecurity to board members and senior leaders?

Seven effective strategies for communicating cybersecurity issues to the board and senior leaders

1. Create a dialogue to engage leadership and build trust

Leadership is about accountability. CISOs and CIOs should provide board members with information that can help them make the best decisions around governance and senior leaders with the intelligence to make optimal management decisions. Ultimately, the stakeholders we spoke with want to elevate the dialogue to help their leaders make informed decisions and set strategic direction. More than providing a briefing on cybersecurity, they want to have a dialogue. Many of our interviewees said their role is to make sure the risk gets escalated to the right level of leadership. A critical early step is to ensure the board and senior leadership agree on the *crown jewel* data and assets that are most in need of protection.

Our interviewees explained that a good report would provide leadership with a better understanding of the organization's current state of cybersecurity, including:

- Threats and vulnerabilities the security team is seeing, as well as the near-term proactive steps being taken to mitigate those threats;
- A clear understanding of how those threats and vulnerabilities could impact business functions;
- Longer-term strategies, objectives, investments, and associated returns on investment (ROI) the team has established to deal with these threats; and
- Progress in achieving the objectives.

This first strategy—establishing a dialogue and building trust—serves as a critical foundation for the other strategies.

Our interviewees said that it takes time to build a deeper understanding of the core elements, and to build the credibility and trust necessary for the board and senior leaders to make decisions based on the security team's recommendations. Some interviewees noted that executives aresometimes skeptical of recommendations around active threathunting—where the security team hires a third party to exploit and identify system weaknesses. The skeptics'

Many of our interviewees said their role is to make sure the risk gets escalated to the right level of leadership. A critical early step is to ensure the board and senior leadership agree on the crown jewel data and assets that are most in need of protection.

rationale is often, *what if we hunt for something and find it? Does it mean we're not compliant? Might our vulnerability be leaked?* Our interviewees said that providing transparency about an organization's specific weaknesses can be uncomfortable, but it is necessary. Many of our interviewees emphasized the importance of being able to freely disclose the nature of the cyber risks an organization faces without having to worry about backlash. The board and management should clearly understand the threats and be able to help develop appropriate mitigation strategies.[6]

> **This first strategy—establishing a dialogue and building trust—serves as a critical foundation for the other strategies.**

If leadership views the CIO, CISO, and their team as more operational and focused only on technology or information risks, the cybersecurity team could be treated as less of a strategic asset. Deloitte's 2019 Future of Cyber survey indicates a growing number of CISOs are starting to report directly to the CEO. This is a positive shift to note, as access and influence are imperative in helping executives prioritize and understand what is needed to propel the enterprise forward in the realm of "cyber everywhere."[7] Regardless of how companies structure the chain-of-command, it is important to ensure the cyber function is senior enough to have line of sight and influence into strategy and operations.[8]

2. Use the power of storytelling and narrative to make it real

CISOs might only address the entire board for a few minutes once a year, or once a quarter. Most CISOs speak to smaller board committees, such as the audit committee, more frequently. That means there is pressure to ensure their presentations are crisp and effective. Storytelling can be more powerful than a PowerPoint when addressing leadership. Many interviewees acknowledged that when they get in front of leadership, they typically use slides to report basic metrics (more on that below) and convey information. They said this is sometimes the least effective and least interesting part of their communication.

How do CISOs, who often have extensive technical background, effectively get their points across? Many of our interviewees—as well as security stakeholders who write about this topic in business literature—suggested using stories to help their audience relate to the issues.[9] Some stakeholders recommend creating a "story inventory" ahead of time, and use it to help illustrate relevant situations.[10] One interviewee from a life sciences organization said he and his team typically prepare for board meetings by building stories around a few recent cyber incidents in the organization. The key, he said, is to describe the incident and make sure to explain the impact it had (or could have had) on the business. Connecting specific incidents with specific business functions can help organization leaders make better decisions around addressing risks and managing processes.

Another strategy is using personas to illustrate how different areas of the business could be affected. For example, showing how a cyber incident might impact a patient, a physician, or a regulator can be an effective technique. Conveying the pressing issues CISOs want to get across in this way can help the board and leadership see the risk landscape through a different lens. Using personas can give CISOs another way to discuss relevant and meaningful strategies across different business functions.

Consider this: The CISO at a life sciences company created internet safety awareness sessions aimed at the families of board members and senior leaders.[11] In a prior role, this CISO had worked for an organization where hackers used social media to find information about the families of company executives and used that information to send a phishing email which an executive opened. Most board members said this example really resonated with them and helped link the cyber risk with the potential impact on the business.

PUTTING A BUSINESS LENS ON TECHNICAL CHALLENGES

An interviewee from a large health system told us, "Don't geek out with senior leaders. Save the technical language for the technology team. When you talk to the board or your CEO, speak the language of business risk." In Deloitte's *Beneath the surface of a cyber attack* study, we reported that boards, executive management, and technology leaders are struggling to connect the dots on a wide range of topics familiarly grouped under the heading of *cyber*.[12] At the core of this struggle is a view that business executives and security professionals seldom speak the same language. Perhaps more importantly, they rarely approach cyber challenges in a way that integrates multiple competencies to create better business context and insight in their cyber strategies.[13] CISOs should have strategies (whether telling stories or using personas) for translating technical risks into a business context.

3. Help board members and leadership understand that a "cyber everywhere" mentality is the new norm

The threat landscape is constantly evolving, which means there is no checklist for every meeting or update. Not only are the bad actors adapting and getting smarter, but the business of health care demands that organizations continually expand their ecosystem. Many life sciences and health care organizations are enhancing mobile apps to better engage consumers, and they are partnering with retailers and nontraditional players. As their organization moves into the cloud and expands its digital footprint, senior leaders will likely have to figure out how to minimize risk. CISOs are emphasizing this point with boards and leadership: Cyber risk management strategy should be a component of business strategy, and it can't simply be delegated to the IT team.

Our interviewees agreed that cyber-risk simulations can help build incident-response muscle memory across the organization. Cyber exercises immerse participants in a simulated and interactive cyber-attack scenario, allowing the organization to stress-test response reflexes, identify capability gaps, and train on and develop advanced preparedness techniques. Given the expanding cyber threats across the health care ecosystem, organizations are expanding these exercises to include other organizations—recognizing that an attack on one can be an attack on all. These more sophisticated exercises amplify awareness among participating organizations, and can effectively illustratethe value of working together to address cyberattacks. Most interviewees indicated that they would like to conduct a cyber-risk simulation every six months, or at least annually. In reality, it's one of many crisis situations for which organizations have to prepare.

CISOs are emphasizing this point with boards and leadership: Cyber risk management strategy should be a component of business strategy, and it can't simply be delegated to the IT team.

4. Explain how the cyber team is collaborating with people inside and outside of the industry

Interviewees agreed they compete with other life sciences and health care companies on market share, building relationships with consumers and providers, and other facets of the business. They don't compete in cybersecurity. The CISO from a large health plan noted, "We appreciate the need for herd immunity. We do business together, so the supply chain is shared: If one of us is weak, we could all be weak." Collaboration among CISOs and their equivalents is a big factor in many cybersecurity strategies. Collaboration can be a combination of official and more informal channels—such as the Health Information Sharing and Analysis Center (H-ISAC), consortia, meetings, and just having other CISOs on speed dial.

Cross-industry collaboration is another important strategy. There is a growing need for businesses and governments to collaborate to leverage learnings and strengths. Some industries are working together to develop strict standards and adherence to strengthen and innovate security. A few of the CISOs we interviewed said they looked to Silicon Valley and other creative hubs to stimulate thinking on cybersecurity innovation. "We talk with some of the big technology companies, and it's clear they have a much more seamless view of IT and the business," said one of our interviewees. "It is just embedded into the company. It IS the business. That mindset is increasingly important for health care organizations."

Technology companies have a seamless view of IT and the business—IT *is* the business. Increasingly, health care organizations are adopting that mindset.

Many of our interviewees said leadership is interested in how the security team collaborates within the ecosystem. Leaders don't want the team to reinvent the wheel if the organization can benefit from others' experience. A CISO we interviewed from a health care organization with a more mature board said that the cybersecurity team often reaches out to the board members' organizations when trying to solve a specific cybersecurity problem. The CISO noted that it is important for teams to understand where the board members are coming from in terms of the culture and practices of their organizations. A few interviewees noted how important it is to collaborate with industry disruptors (such as big technology companies as well as newer startups) that are beginning to influence how life sciences and health care organizations think about their businesses and the way they engage with consumers.

GETTING BUY-IN THROUGH WARGAMING

The Deloitte 2019 Future of Cyber survey found that only 32 percent of C-level executives say their companies conduct cyber wargaming exercises to prepare them for real-world incidents. Wargaming involves the various business leaders in a plausible scenario and creates collective buy-in for everyone's role in cybersecurity. Because the threat landscape changes rapidly and responses cannot be perfectly scripted, cyber wargaming is recognized as a leading strategy to get ahead.[14]

5. Use metrics to quantify risks, elevate the discussion in dollar terms, and connect it back to the business

While all of our interviewees agreed that metrics were important, there was general consensus in our interviews that leadership is most interested in knowing:

- What are the risks we are facing?
- What is the cybersecurity team doing about it?
- Does the team have what it needs to make the right decisions and act quickly?

Our interviewees didn't cite one standardized framework for quantifying risk or risk management, though many mentioned the National Institute of Standards and Technology (NIST) framework as a helpful starting point. But to make it easier for leaders to understand, cyber risk should be viewed as a business decision rather than a technical one. CIOs and CISOs should quantify their cyber risk in financial terms for leadership and empower executives to make informed decisions. Using financial modeling, companies can adopt approaches for estimating both the direct and intangible costs associated with cyber risk. This kind of modeling can provide greater clarity to support investment decisions around protecting the most valuable assets.[15]

Despite the lack of perfect metrics, or a standardized way to quantify risk, the professionals we interviewed agreed that a metrics-driven approach is important to clearly connect the dots back to the mission of the organization, and back to specific business functions. A major theme was the importance of building updates based on a few key metrics that can be tracked over time. This can help illustrate progress and the evolving landscape.

All of our interviewees said they use maturity models in their presentations to boards and leadership. Typically, these models show quarterby- quarter trends to demonstrate program maturity and outline the major initiatives under way. However, presenting a trend can be difficult, according to some interviewees. The ever-evolving threat landscape might look worse on a given metric. It's critical to provide leadership with the right context to understand how maturity levels are evolving with targets. While a few of the organizations we spoke with had mature boards in terms of cybersecurity, a health plan board member said some members still get nervous when the same risks show up in report after report. Less mature boards may get into a mental framework that thinks along the lines of: *"I thought this was taken care of … why is this still showing up?"*

Ultimately, interviewees said their role is to help make leadership comfortable with the reality that everything cannot be protected equally. Organizations should have clear agreement and an understanding of which data is most critical to the enterprise, where it resides, how it is collected and shared, and the potential impact if it is compromised.

6. Be prepared to answer and defend questions related to cybersecurity investments

Company leaders often ask CISOs how much the organization should invest in cybersecurity. Our interviewees said it was necessary to emphasize that cybersecurity is an ongoing challenge and a moving target, and no dollar amount can make the risk disappear. There are some general benchmarks, but investment decisions vary based on the maturity of the overall program.

The subject of ROI is complicated for cybersecurity, our interviewees said. Actuaries who work in cybersecurity insurance build in certain assumptions. The numerator is typically clear, but the denominator often isn't. Many of our interviewees said that the biggest variables—brand reputation value, a compromise in patient safety or trust, and potential legal costs—are harder to quantify. Deloitte's *Beneath the surface of a cyberattack* report describes 14 impact factors that business leaders should consider when preparing for cyber incidents.[16] These factors range from well-known impacts that have direct costs commonly associated with breaches to more far-reaching, intangible costs that can be difficult to quantify, such as loss of intellectual property, data destruction, or credit-rating impact.

Interviewees noted that while funding usually isn't a problem, there are some concerns that leadership and board members could become numb to the constant headlines and discussions of threats. Many organizations have had cyber incidents, but they might have had minimal financial implications. Some of the CISOs and CIOs said it is important that they effectively explain how the threat landscape is evolving. The metrics they report on and the context they provide should strike the right balance between the threat landscape and what they can do to manage the risk.

Cybersecurity is likely to remain an integral function for life sciences and health care organizations. This means organizations will need to continually improve capabilities as threats evolve in scope, technique, and sophistication.[17] Most organizations have just scratched the surface when it comes to cybersecurity benchmarking. As the field evolves, organizations could create benchmarks such as:[18]

- Maturity score by NIST domain;
- Cybersecurity spending as a percentage of IT spending, as well as per full-time equivalent (FTE); and
- Number of cyber risk FTEs as a percentage of information security and total IT personnel.

SOME CYBERSECURITY COMMUNICATIONS ISSUES TRANSCEND INDUSTRIES

In previous research, Deloitte surveyed and interviewed CISOs and cybersecurity executives in the financial services industry (FSI).[19] Some of these findings were similar to what we saw in life sciences and health care. The FSI executives said their companies had dramatically increased cybersecurity budgets over the past few years, and they expected that trend to continue in the near term. But a number of FSI interviewees acknowledged the pace of cybersecurity budget increases might be unsustainable in the long term.[20] Similar to FSI, the CISOs and CIOs we interviewed acknowledged that they will need to pay particular attention to managing a solution's life cycle. Longer term, at some point CISOs will have to start making hard choices on spending priorities. This should be based on a true cybersecurity game plan that is aligned with the company's business and technology strategies.

In both areas of research, the cybersecurity executives noted that the onus of measuring and communicating the ROI by demonstrating quantitative and qualitative benefits of cyber investments is paramount to ensuring they are seen by the board and leadership as being good stewards.

7. Regularly assess and discuss future talent models and their potential impact on the organization

Attracting and retaining skilled talent was a top-of-mind concern for many of our interviewees, and it was also a priority for their boards and senior leaders. More than three-quarters of CISOs surveyed in a recent Deloitte CISO labs report said they lacked the skilled resources and effective team structure to support their priorities.[21]

For CISOs and their teams, diversity in experience is key. Our interviewees emphasized the need for resources who understand the technical side as well as the organization's business functions. Many CISOs and CIOs we spoke to told us part of their job is to grow talent, but noted that traditional recruiting and retention models were failing them. They said they are working with their organizations and the board to evolve to newer models.

One popular strategy is to recruit people who have business and communication skills, and train them on the technical side.

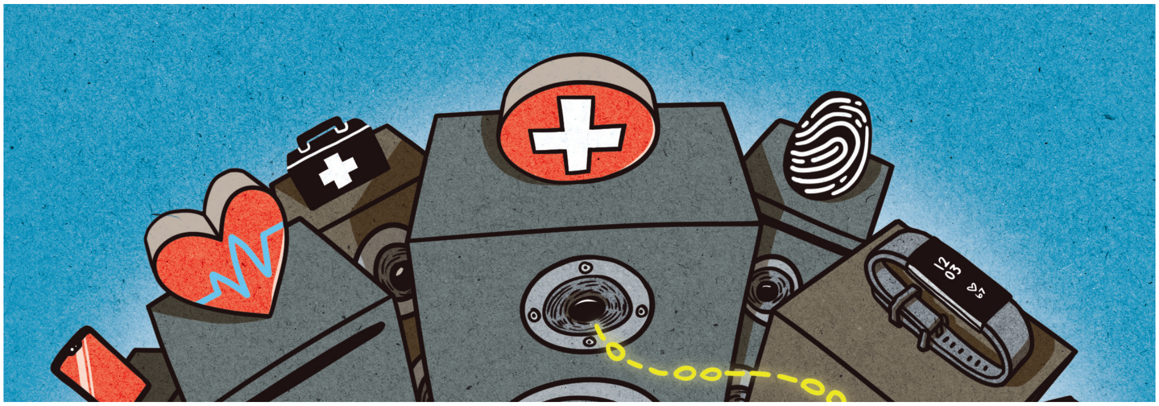
Many of our interviewees are trying different strategies to help train people to apply skills in a real-world setting. The bad actors in cyber tend to be young and typically do not have degrees. To ensure counter-cyber teams have the right skills to combat the bad actors, some organizations are paying less attention to formal education—opting instead to train on the job. Some interviewees noted that university recruiting is still occurring, but university courses are not always as current as they would like, given how rapidly the cyber-threat landscape is evolving.

One popular strategy is to recruit people who have business and communication skills, and train them on the technical side. The technical elements of cybersecurity are sometimes easier to teach than the skills needed to effectively communicate with leadership. Cyber team members should be able to translate technical information into business terms and prioritize risk mitigation efforts.

Here are some strategies we put together from our interviews—supported by secondary literature research—to tackle the talent dilemma:

- **Explore partnerships with universities and professional organizations to enhance team skill sets.** Identify leadership potential in nontechnical employees and help them become well-versed in cyber risk.[22]
- **Hold cyber "war games" for staff.** These simulated scenarios are designed to test the readiness of an organization for specific cyber vulnerabilities and also provide employees with hands-on experience.[23]
- **Consider nontraditional talent.** Some organizations are recruiting law school graduates for short-term stints. The graduates get technical training and can move on to careers in cybersecurity insurance or cybersecurity law. One CISO mentioned his organization was interested in recruiting recent English literature majors who were willing to get technical training on the job.
- **Reward employees for knowing the business.** Our interviewees noted that to attract and retain millennials and younger generations, continuous learning and growth opportunities such as providing avenues for rotation and movement within the company are critical.

Bringing a business perspective to cyber risk



EFFECTIVE COMMUNICATION WITH the board and leadership is critical for CISOs' and CIOs' success in helping the organization mitigate and manage the rapidly evolving threat landscape. The CISOs we interviewed acknowledged the challenges of not being decision-makers, but being responsible for helping the leadership and board make the right decisions. The strategies we outlined, based on our research, are a guide for life sciences and health care CISOs, leadership, and boards as they refine and evolve their cyber risk-management programs. Periodically, organizations can ask themselves:

- Is there an active and effective dialogue among the board, leadership, and the cybersecurity team about where the value is created in the organization, where the critical assets are, and what is their vulnerability to key threats?
- Does the CISO have the trust of the leadership and the board so that everyone is in sync on critical decisions? Are we an organization that rewards openness and transparency?
- Are we adapting to the changing ecosystem—and are we integrating cybersecurity into a true enterprisewide risk approach?
- Are we incentivizing openness and collaboration by building strong relationships with peers, partners, competitors, and other industries?
- Are we examining and paying appropriate attention to our future workforce? Are we doing what we need to do to recruit and retain top talent?
- Are we looking at new ways of investing in cyber to help us mitigate risk?

One constant in the cybersecurity team's communications is to help the board understand that traditional boundaries in life sciences and health care are no longer valid. The business and technology innovations that companies are adopting in their quest for growth, competitiveness, and cost optimization are, in turn, leading to heightened levels of cyber risks. Bad actors exploit weaknesses that are byproducts of business growth and technology innovation. Such weaknesses could be related to mergers and acquisitions, new customer services, supply chain models, applications and mobile tools designed to engage consumers, and new technologies purchased to help improve efficiency and control costs. Being too risk-averse is not an option, and cybersecurity stretches beyond internal operations.

As cyber threats evolve, so too must CISOs' relationship with the board and senior leaders. In the future, CISOs may incorporate more predictive analytics into their metrics and trending. This could help guide discussions with the board and leadership around how much risk an organization is carrying and whether existing strategies are enough to address the risk. Ideally, organizations will use these types of tools to assess specific risk areas and assign them a value, which can help answer ROI questions.

Finally, our research highlights the importance of the CISO's role in bringing a business perspective to cybersecurity risk. Our interviewees acknowledged that helping board members and leadership understand how cybersecurity risks connect to business functions is a journey. In a health care system increasingly driven by digital technologies and information flow, CISOs want leaders to understand that cyber-threat management is more than just a strategic imperative. It is a fundamental part of the business.

SOME CYBERSECURITY COMMUNICATIONS ISSUES TRANSCEND INDUSTRIES

The Deloitte Center for Health Solutions conducted a series of interviews with 18 life sciences and health care stakeholders from December 2018 through March 2019. These stakeholders were from organizations that included a mix of life sciences (biopharma and medical device companies), health plans, and health systems. The interviewees included chief information security officers, chief information officers, and a small number of board members and chief risk officers.

We also interviewed specialists and leaders from Deloitte's cybersecurity and advisory practices, and used findings from:

- A 2018 Deloitte survey of chief financial officers from health care organizations on the topic of enterprise risk and compliance;
- A 2018 Deloitte survey and series of interviews from CISOs from the financial services industry; and
- A 2019 Deloitte survey of C-level executives who are responsible for cybersecurity in companies with at least US$500 million in annual revenue (note that this survey included many industries beyond life sciences and health care).

We also conducted a literature search.

Endnotes

1. Erin Dietsche, “11 cybersecurity tips from the first federal chief information security officer,” *MedCity News*, February 13, 2019.
2. Khalid Kark, Caroline Brown, Jason Lewris, *Bridging the boardroom’s technology gap*, Deloitte University Press, June 29, 2017.
3. Ibid.
4. Tony Kontzer, “C-suite cybersecurity awareness may be the key to taking a bite out of breaches,” RSA Conference, July 19, 2018.
5. Brad Lindemann, “Why every public company should have a cyber security expert on its board,” LinkedIn, March 22, 2019.
6. Deloitte, *Governance in focus: Cyber risk reporting in the UK*, March 2018.
7. Deloitte, *The future of cyber survey 2019*, 2019.
8. Ibid.
9. Frederick Scholl, “Better security through storytelling,” CSO Online, January 30, 2017.
10. Ibid.
11. Christie Terrill, “What you need to know about cybersecurity and social media,” *Forbes*, April 28, 2017.
12. Deloitte, *Beneath the surface of a cyber attack: A deeper look at business impacts*, 2016.
13. Ibid.
14. Deloitte, *The future of cyber survey 2019*.
15. Deloitte, *Beneath the surface of a cyber attack*.
16. Ibid.
17. Jim Eckenrode and Sam Friedman, *The state of cybersecurity at financial institutions*, Deloitte Insights, May 21, 2018.
18. Ibid.
19. Ibid.
20. Ibid.
21. Taryn Aguas, Khalid Kark, and Monique François, “The new CISO: Leading the strategic security organization,” *Deloitte Review* 19, July 25, 2016.
22. Ibid.
23. Alexandria Nelson, “Are you taking gamification seriously? Four reasons to implement it now,” Interact, April 13, 2018.

About the authors

AMRY JUNAIDEEN, managing principal, is the leader of Deloitte's Risk & Financial Advisory practice for Life Sciences and Health Care. Junaideen has more than 26 years of diversified global experience in the private and public sectors, having served large multinational and public sector clients on many risk management and information technology–related initiatives. His specialties include risk management, systems integration, internal controls transformation, and talent management. Junaideen has had numerous client and practice leadership roles, having worked on Pfizer, Amgen, Beyer Pharmaceutical, Genzyme Corporation, Astra Zeneca, the Centers for Medicare & Medicaid Services, and the Australian Regional Public Health System. He was also the National and Global Security & Privacy leader for life sciences. Connect with him on LinkedIn at www.linkedin.com/in/amry-junaideen-23a775/.

CASEY KORBA is the health policy manager for the Deloitte Center for Health Solutions, where she provides comprehensive regulatory and policy analysis and conducts research in areas including valuebased care, emerging technology, and consumer transformation. Prior to Deloitte, Korba served as the director of clinical affairs and strategic planning for America's Health Insurance Plans (AHIP). She has an MS from American University. Connect with her on LinkedIn at www.linkedin.com/in/caseykorba/.

Acknowledgments

PROJECT TEAM

Bushra Naaz and **Kiran Vipparthi** provided extensive background research, interpreted findings from the primary and secondary research, and assisted with the writing.

The authors would like to thank **Carlos Amaya**, **Ajay Arora**, **Hector Calzada**, **Michael Cunning**, **Jason Frame**, **John Gelinne**, **Terry Hisey**, **Kyle Johnson**, **Russell Jones**, **Jimmy Joseph**, **Matthew Kates**, **Steve Livingston**, **John Lu**, **Andrew Morrison**, **Larry Samano**, **Kelly Miller Smith**, **Heather Varner**, and **Sean Wright** for their expertise, support, and guidance.

The authors would also like to thank **Samantha Gordon**, **Lauren Wallace**, **Sarah Thomas**, and the many others who contributed their ideas and insights to this project.

About the Deloitte Center for Health Solutions

The source for fresh perspectives in health care: The Deloitte Center for Health Solutions (DCHS), part of Deloitte LLP’s Life Sciences and Health Care practice, looks deeper at the biggest industry issues and provides new thinking around complex challenges. Cutting-edge research and thought-provoking analysis give our clients the insights they need to see things differently and address the changing landscape. To learn more about the DCHS and our research, please visit www.deloitte.com/centerforhealthsolutions.

Contacts

Amry Junaideen
Managing principal
Life Sciences & Health Care for
Risk & Financial Advisory
Deloitte & Touche LLP
+1 571 766 7178
ajunaideen@deloitte.com

Sarah Thomas, MS
Managing director
Deloitte Center for Health Solutions
Deloitte Services LP
+1 202 220 2749
sarthomas@deloitte.com

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Ramani Moses, Blythe Hurley, Abrar Khan, and Rupesh Bhat
Creative: Ramani Moses, Blythe Hurley, Abrar Khan, and Rupesh Bhat
Promotion: Alexandra Kawecki
Cover artwork: Dongyun Lee

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.