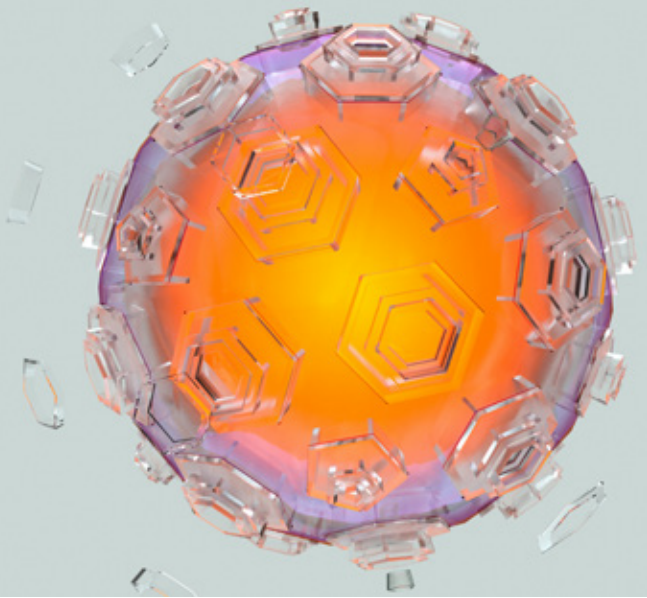
From Reaction to Resilience

How Healthcare Services CEOs and Boards Can Rethink Cybersecurity



Healthcare payers and providers are a top target for cyber-breaches, events that are only increasing in severity and impact. Indeed, 2024 was the worst year for breached health-care records, affecting 81% of the U.S. population. While cyber breaches have significant financial and operational implications, they also have impacts on human life and consumer trust that are much harder to repair.

To dig deeper into how healthcare services organizations are addressing consistent cybersecurity threats, we spoke with five cybersecurity and technology leaders in the sector. This article, based on their unique insights as well as our extensive experience as advisers to top industry cybersecurity leaders, looks at the top-of-mind priorities for healthcare services CISOs and the broader C-suite, how CEOs and boards can find the right cyber leader, and what leadership capabilities are most critical for cyber leaders today and in the future.

Navigating the cybersecurity threat landscape

Provider and payer organizations are concentrating efforts on a few key strategic areas.

Obtaining sustainable investment in cybersecurity programs. It's not uncommon for organizations to ramp up their focus and budget on cybersecurity in the wake of a breach. Yet, as time passes, dedication to cybersecurity programs often subsides and these organizations slash investments in those programs, leaving themselves open to vulnerabilities.

To maintain sustained investment and support in cybersecurity programs, CISOs should clearly and concisely explain to executives and the board the connection between cybersecurity and ongoing technology investment, and the patient and business impacts.

"If you're not connecting everything to patient care, then you won't have a successful program and won't get the budget," said one cyber leader we spoke with. "Nobody cares that you don't have an endpoint detection and response solution, but they do care that patient care is affected when computers are down for a month because of ransomware."

Reevaluating third-party risk management practices. The 2024 Change Healthcare breach revealed a significant lack of visibility and awareness from cybersecurity leaders around the extent of their risk exposure be it operational, administrative or financial via direct or indirect vendor relationships. In fact, nearly 40% of all U.S. medical claims clear through Change.

> **"If you're not connecting everything to patient care, then you won't have a successful program and won't get the budget."**

Several cybersecurity leaders we spoke with are now heavily investing in third-party risk management programs to ensure they have complete and regularly updated views of risk — and a plan. For example, cyber leaders might establish regular vetting protocols to review their current list of vendors and understand whether these vendors have contingency plans in place, what their sourcing route looks like, and whether they have back-up plans for a security breach.

More people are recognizing that "I hope it doesn't happen to me" is no longer a viable tactic, one cybersecurity executive for a top healthcare services organization told us. "They're aware that it's likely to happen," he said. "Now it's a matter of figuring out how big a breach it is, and how well prepared you are to weather the storm."

Improving visibility and control across the technology estate. Payer and provider organizations often pursue M&A as part of their growth strategies. However, this approach can lead to a patchwork of unintegrated technology platforms and associated security challenges. The most common issues are outdated security measures that reduce visibility and control across the technology estate, leaving organizations vulnerable to attack.

In many cases, the acquiring company takes a watered-down approach to cybersecurity integration, focusing only on tasks such as making sure multifactor authentication is in place. And the acquired companies are not much better.

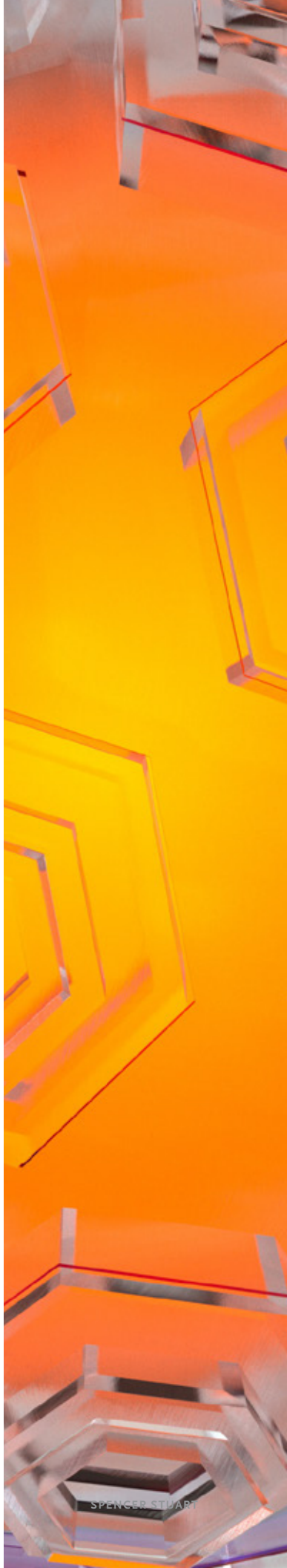
Jorge DeCesare, former chief technology risk officer and global CISO at Kaiser Permanente, recommends performing a pass-fail assessment on any company being acquired to see how well they score against the NIST cybersecurity framework.[1] This will provide fundamental insight into that company's cybersecurity program and posture.

Cyber leaders with M&A experience are better equipped to navigate these hybrid legacy environments and support technological modernization efforts amid integration. One leader described a transformation plan that delivers short-term wins (such as fixing security deficiencies) while pursuing a longer-term strategy to enable consistent and standardized processes that address enterprise-wide problems around full system visibility and integration.

Collaborating and sharing information. Several interviewees highlighted the value of participating in information networks both in and out of industry. Information sharing can help cyber leaders better understand the needs and challenges of multiple stakeholders — from vendors and other third parties to providers and patients — so they can build more effective controls.

Information sharing can help cyber leaders better understand the needs and challenges of multiple stakeholders — from vendors and other third parties to providers and patients — so they can build more effective controls.

1 The NIST cybersecurity framework is a set of guidelines developed by the U.S. National Institute of Standards and Technology to help organizations identify, respond to and mitigate cybersecurity risks.



A broader perspective also supports continuity planning by ensuring critical business relationships and services are protected — even if a breach occurs. And with the expected proliferation of AI-driven threats, such as phishing emails and deep fakes, cross-sector collaboration is even more urgent for helping companies identify and mitigate attacks.

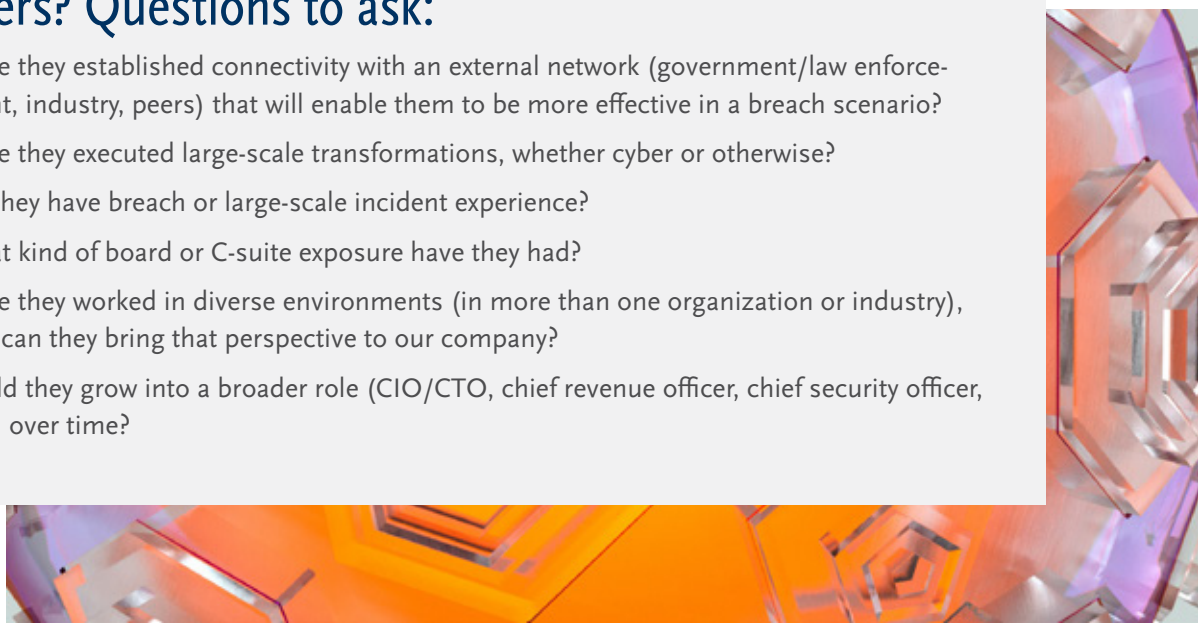
Broadening the cyber talent search: Why it's worth looking beyond healthcare services

For CEOs and boards either seeking new cybersecurity leadership or considering whether they have the right leader in the seat, recruiting from within healthcare services offers certain advantages. Our analysis of the cybersecurity leaders in the top 25 largest U.S. healthcare services organizations shows that 75% came from within industry, compared with 49% of Fortune 100 CISOs. Recruiting from within the industry or promoting from within the company ensures that your cyber leader has a nuanced understanding of the industry's complexities, such as its strict regulations and mission-driven approach to business.

At the same time, healthcare CEOs and boards can benefit from widening their aperture when looking for talent. Given that cybersecurity skills are generally transferrable across industries, there is value in learning from (and hiring from) other regulated industries where cybersecurity maturity is more advanced. As one healthcare CISO said, "My pitch to the board is that we shouldn't compare ourselves to other health systems; we have to compare ourselves to the best in cyber."

How should CEOs and boards assess potential cyber leaders? Questions to ask:

- Have they established connectivity with an external network (government/law enforcement, industry, peers) that will enable them to be more effective in a breach scenario?
- Have they executed large-scale transformations, whether cyber or otherwise?
- Do they have breach or large-scale incident experience?
- What kind of board or C-suite exposure have they had?
- Have they worked in diverse environments (in more than one organization or industry), and can they bring that perspective to our company?
- Could they grow into a broader role (CIO/CTO, chief revenue officer, chief security officer, etc.) over time?



Below are examples of what healthcare services can learn from other industries:

- Leaders in industrial and manufacturing have learned how to maintain uptime and resilience during a cyber breach while keeping costs down. This skill is similarly valuable in healthcare, where minimizing system downtime is critical to delivering patient care.
- Financial services, like healthcare, is highly regulated, which is a reason cybersecurity became a board-level priority early on. Healthcare services can follow suit by making cybersecurity a regular topic in executive discussions and connecting the dots between cyber risk mitigation and strong patient satisfaction and health outcomes.
- Cyber leaders in consumer-oriented companies link the cybersecurity mission to the brand, product or marketplace by highlighting how it builds customer trust. Provider and payer organizations can also connect the dots between cybersecurity and patient trust. They can also emulate best practices around consumer data privacy and protection.

Redefining cybersecurity leadership

Despite growing board-level recognition of cybersecurity as a strategic priority, many payer and provider organizations still lack cyber leaders who translate intent into action. In fact, many healthcare organizations don't recognize until after a breach occurs that their CISO might be a fantastic technical resource but is unable to effectively communicate with executive leaders about what risks exist and how to address them.

That's one reason organizations are beginning to redefine the profile of cyber leadership.

"The archetype of the cyber leader is evolving toward someone who is an effective communicator," said Daniel Nutkis, CEO at HITRUST, a provider of risk management and compliance assessments and certifications. "They need to be able to influence, collaborate with various stakeholders, and talk about cybersecurity in business and operational risk terms."

Below we look at how the role of a CISO is changing and the core capabilities needed in the current landscape.

Collaboration and influence

A large part of effective influence comes down to the style of the individual leader, but a top-down approach to positioning cybersecurity is also critical. Cyber leaders need a seat at the leadership table so they can provide guidance on cyber considerations related to business, technology, operations and risk. Access also gives them visibility into the board and CEO and the business agenda and strategy, helping to develop an environment where cyber is much more than a "back-office" function or cost center.

Collaboration is also critical given the interdependence and complexity of systems, networks and functions inherent in healthcare services organizations. Collaborative CISOs present the risks associated with a product or project, and ask, *How can we work around this?* Then they help find a path forward that balances risk and resilience and the inputs of internal stakeholders.

"Any environment you're working in is highly matrixed," said David Lundal, CIO at Children's Minnesota. "To be effective, you need the ability to work across organizational lines."

Strong communication skills

Every cyber leader today is presenting to the board with some degree of frequency; providing clear, concise updates on the maturity of a cyber program is table stakes.

Effective CISOs speak the language of risk, technology and business and clearly communicate the potential impact of risk on the organization to the board so they can make informed decisions. Furthermore, leading CISOs are spearheading the topic of residual risk with the board. Strong cyber leaders in healthcare are also adept at communicating the vital connection between cybersecurity and patient care.

"You can't hire a gearhead," one healthcare services cyber leader explained. "You need someone who can distill things down into a story that a layman can understand, because the majority of folks you interact with don't know anything about security."

Savvy in technology and business

Differentiated cyber leaders display a balance of technical depth and business acumen. They are familiar with different technologies and their potential applications so they can ask the right questions and ensure they don't miss risk — and business — implications. Artificial intelligence, for example, can accelerate the velocity and sophistication of cyber attacks, both internally and externally. Cultivating knowledge around these threats, such as email phishing or deepfakes, can help leaders design more effective controls.

At the same time, strong cyber leaders know how to leverage AI within their organization to increase efficiency in administrative duties like billing and clinical use cases, while also implementing proper safeguards.

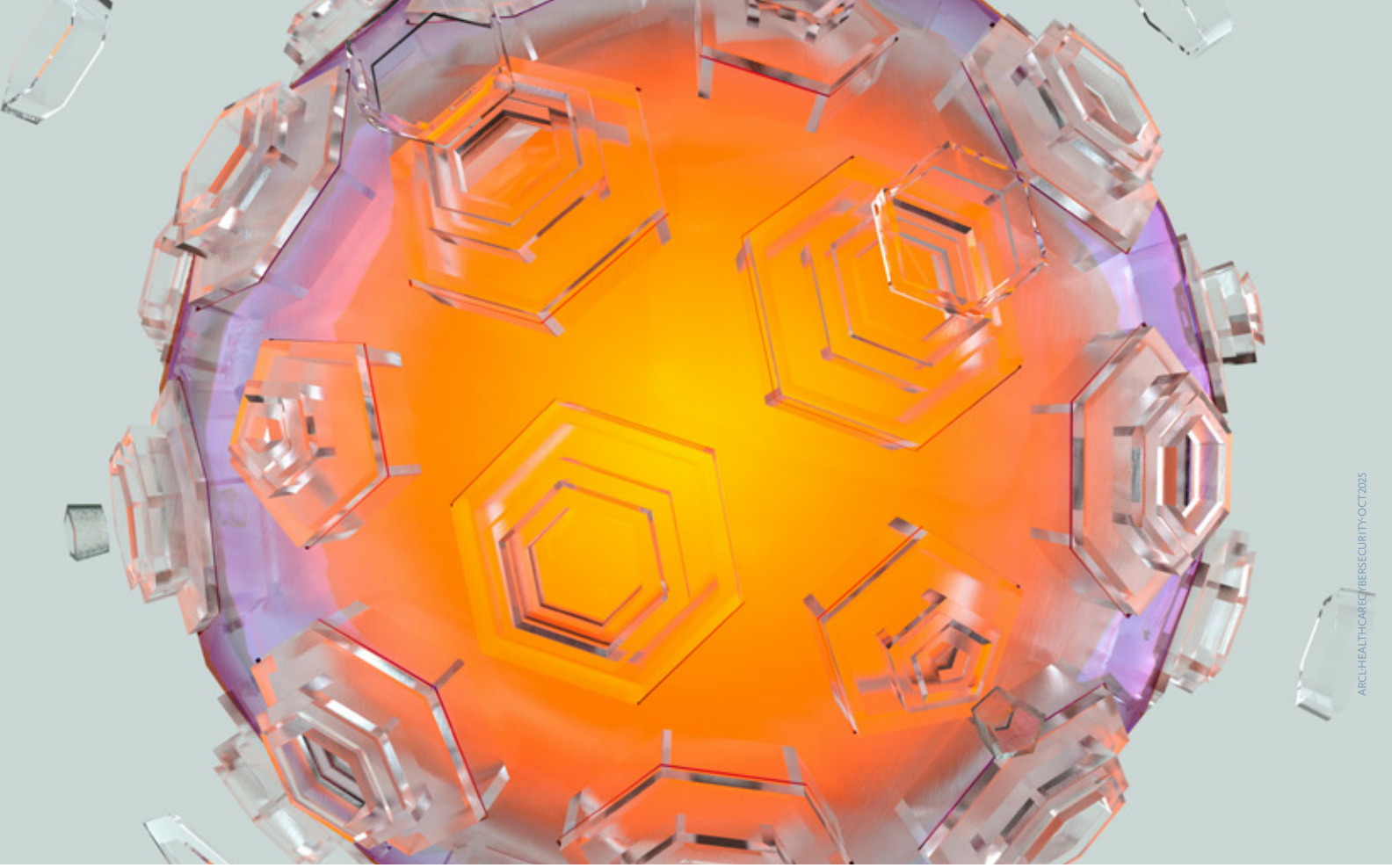
> **"You need someone who can distill things down into a story that a layman can understand because the majority of folks you interact with don't know anything about security."**

Building cyber resilience

As healthcare services organizations face increasingly complex and volatile environments, CEOs and boards must recognize that cyber resilience is not just a technical goal — it's a business imperative. Cyber leaders who can influence strategy, communicate risk in business terms and prioritize such risks are best positioned to make cybersecurity part of the organization's DNA.

This culture shift needs to come from the top down, with CEOs and boards looking at their own preparedness when assessing the organization's cyber resilience. By receiving ongoing learning and development training and building skills in critical knowledge areas such as cybersecurity and AI, boards can improve their oversight into cybersecurity.

By aligning cyber leadership with business strategy and the board agenda, healthcare services organizations can move from reactive defense to proactive resilience — protecting patients, restoring trust and preparing for the future.



About Spencer Stuart

At Spencer Stuart, we know that leadership has never mattered more. We are trusted by organizations around the world to help them make the senior-level leadership decisions that have a lasting impact on their enterprises, on their stakeholders and on the world around them. Through our executive search, board and leadership advisory services, we help build and enhance high-performing teams for select clients ranging from major multinationals to emerging companies to nonprofit institutions.

Privately held since 1956, we focus on delivering knowledge, insight and results through the collaborative efforts of a team of experts — now spanning more than 60 offices, over 30 countries and more than 50 practice specialties. Boards and leaders consistently turn to Spencer Stuart to help address their evolving leadership needs in areas such as senior-level executive search, board recruitment, board effectiveness, succession planning, in-depth senior management assessment, and many facets of culture and organizational effectiveness, particularly in the context of the changing stakeholder expectations of business today. For more information on Spencer Stuart, please visit **www.spencerstuart.com**.

Authors

Ian Finlay (Los Angeles)
Kate Hannon (New York)

The authors wish to thank Ingrid Stiver for her invaluable contributions to this piece.