HEALTH CARE PAYERS, PROVIDERS, SYSTEMS & SERVICES

Cyber Attacks Are Inevitable in Health Care. Patients Don't Have to Pay the Price.

By Russell Schaefer, Tom Retelewski, Adrian Ciuffetelli, and Tad Roselund

ARTICLE MARCH 09, 2026 12 MIN READ

Just as the human body can't block every germ, health care organizations can't block every cyber attack. Yet the fallout from breaches—financial losses, reputational damage, and, most critically, the risk to patient safety—is often far worse than it needs to be. That's because most organizations treat cybersecurity as a purely technical challenge, best left to IT. But cyber

resilience is not an IT problem. It's a strategic imperative whose effectiveness rises or falls with board of directors' oversight.

An Enterprise Initiative

Achieving true cyber resilience is an all-hands endeavor. It requires a health care organization to take a holistic approach that sets clear recovery priorities, drives cross-functional coordination, rigorously tests response plans, and ensures vendors meet core resilience expectations. It's a big shift in mindset and methods—one that the board is uniquely qualified to oversee, with its enterprise-wide view, authority to balance tradeoffs, and accountability for risk.

So far, however, few boards are, well, onboard. Just 27% of boards regularly discuss cybersecurity, according to a BoardEffect survey. Yet the need for true cyber resilience has never been stronger. As health care becomes more digital and interconnected, a single breach can ripple far and wide. The 2024 ransomware attack on Change Healthcare, which processes 15 billion health care transactions annually, showed how fast disruption can spread. A survey conducted by the American Hospital Association found that 74% of US hospitals reported direct patient impact, including delays in treatment, and 60% took weeks to months to fully recover.

Moreover, cyber incidents are a growth industry—highly organized, well-funded, and increasingly focused on health care. According to the Federal Bureau of Investigation's 2024 *Internet Crime Report*, no other critical infrastructure sector faced more cyber threats (which included data breaches and ransomware incidents) in 2024.

Many factors make health care an attractive target. (See Exhibit 1.) For one thing, health data is valuable. In an interview with CNBC, cybersecurity researcher Jeremiah Fowler noted that medical records are worth four times as much as social security numbers. In addition, many organizations still rely on legacy IT systems, leaving them more susceptible to attacks. And as an industry, health care lags in cyber maturity. A 2025 survey conducted by BCG and the research firm GLG found that just 13% of health care organizations have achieved an advanced maturity level, compared with 29% of technology companies and 22% of banks.

EXHIBIT 1

Why Health Care Is a Prime Target for Cyber Attacks

Source: BCG analysis.
[1]Susan Caminiti, "Why UnitedHealth, Change Healthcare were targeted by ransomware hackers, and more cybercrime will hit patients, doctors," CNBC, March 15, 2024.
[2]Puja Mahendru, *The State of Ransomware in Healthcare 2025*, Sophos, July 30, 2025.
[3]Itai Greenberg, "Healthcare attacks are increasing: Why zero trust will prevent care disruptions," Check Point Software Technologies, May 20, 2023.

The question is no longer if disruption will occur but how prepared organizations are to maintain patient care and core operations when it does. Boards that ensure cyber resilience planning, resources, and accountability not only reduce risk but also protect patients, preserve trust, and strengthen the future of health care.

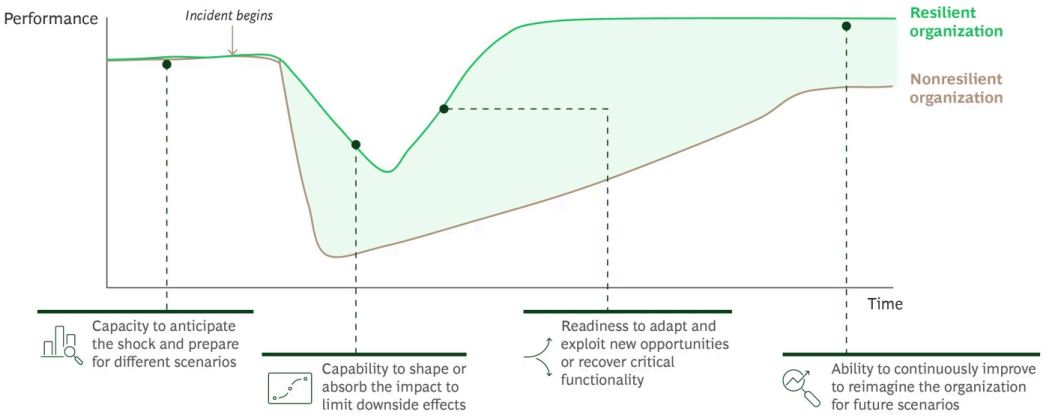
The Board's Expanding Role

To get cyber resilience right, boards need to ask management hard, probing questions about preparation and response, and they should hold leaders accountable for making it a strategic priority. Boards need to push management to identify how systems and business silos interact, how best to sustain operations after an incident (for example, by prioritizing the most critical systems for protection and restoration), and how to adjust the resilience strategy and investment in response to evolving threats, such as AI-driven attacks, which now account for one in six breaches.

It's no simple effort, but the work pays off not only by speeding an organization's recovery from an incident and minimizing harm to patients, reputation, and the bottom line but also by hardening the organization against future attacks. (See Exhibit 2.)

EXHIBIT 2

Recovering from a Cyber Incident Often Takes Longer Than Expected—Risking Patient Care



Source: BCG analysis.

Savvy boards integrate cyber resilience topics into their agendas, risk and audit committees, and governance charters. They ensure that board members have the right expertise and training. But most important, they shift discussions on cyber resilience from technical updates to strategic oversight.

In our experience, boards can start this discussion—and spark the development of a smart, effective resilience strategy—by asking management:

- Which systems and services are most critical for patient care, directly and indirectly? What are we doing to protect them?
- How secure is our value chain? Can care continue if a core supplier is compromised?
- When was the last time we tested and validated our enterprise-level, cross-functional response plan? What did we learn? How have we applied those lessons?
- If we were hit by a cyber or ransomware attack tomorrow, how long would it take to restore critical patient services—and how do we know that?
- How are we ensuring that our cybersecurity investment strategy remains aligned with our most critical risks and vulnerabilities (and with the latest attack methods)?
- Are resources and capabilities aligned for a rapid, coordinated response that cuts across functions? How can we break down silos to streamline and speed decision making?

Five Dimensions That Shape Cyber Resilience

Boards' goal of asking questions should be to surface the organization's true pressure points—and identify the most effective responses when everything can't be protected at once. The idea is to develop a sharper view of where resilience must be built in, where tradeoffs are acceptable, and how the organization will operate under stress. With that insight, boards and management can move to the practical work of shaping a focused resilience strategy.

Such a strategy should optimize an organization across five critical dimensions of preparedness.

STRATEGY AND AMBITION

Boards should link cyber resilience to what matters most. They should ensure the organization establishes strategic clarity about what is truly mission critical: what systems must stay up when a cyber attack happens. Gaining strategic clarity starts with identifying the clinical services the organization simply can't afford to lose—and any digital and operational dependencies. It also means being explicit about how long each service can realistically tolerate downtime and what viable backup strategies, if any, are available.

> "Strategic clarity starts with identifying the clinical services the organization simply can't afford to lose.

Once these mission-critical elements are defined, resilience stops feeling like an abstract IT goal and becomes tied directly to patient safety and business continuity. That shift gives the board firmer ground to stand on as it challenges assumptions, weighs tradeoffs, and pushes the organization—including any management silos—toward better preparedness.

Boards can also set the tone by reinforcing that resilience isn't just an IT responsibility—it needs C-suite ownership, clear escalation pathways (processes for raising issues to the right decision makers), and a place in major enterprise decisions, including capital investments, digital modernization, and how GenAI is deployed.

And to govern effectively, boards should press for real-time metrics that reveal detection and response performance, the readiness of clinical and operational teams, the maturity of recovery capabilities, and the residual risk across internal and third-party systems. With the right visibility, oversight becomes an always-on, always-informed governance practice that aligns the entire organization around protecting patient care.

CROSS-FUNCTIONAL CAPABILITIES

Coordinating functions across the enterprise is critical because when a cyber attack hits, it never stays neatly contained. Clinical workflows slow, operational pressures spike, regulatory clocks start ticking, and communications demands escalate—often all at once. That's why the most resilient organizations make cross-functional coordination a muscle they build on purpose.

Boards should encourage management to create clear crisis roles across the enterprise. Crisis roles are temporary roles that an executive might assume during a cyber incident. For example, the head of risk might assume the role of incident program leader. A communications leader might be assigned to handle all communications related to the incident. Taking this step ensures that clinical leaders can prioritize services and authorize safe manual workarounds; operations teams can manage patient flow and diversion decisions; cyber teams can restore systems in the right clinical sequence; and communications, legal, and supply chain teams can execute their responsibilities without hesitation.

Simulations determine if, indeed, functions work together at critical points. Regular downtime drills, multisite scenarios across campuses, and red-team threat emulations uncover gaps no tabletop discussion could. Preparation and practice also help stem the cost of a data breach. Organizations with high levels of incident-response planning and testing saved some $1.5 million, compared with those that had low levels, according to a report by the Ponemon Institute and IBM Security.

OPERATIONS

Every organization wants to believe that it's ready for an incident. But turning a crisis strategy into seamless execution is hard. Often, the truth becomes clear in the first hour of a real disruption. Boards can help by insisting that readiness be something the organization can show, not simply assert.

Demonstrating readiness starts with preparing recovery "runbooks" that hold up under pressure. Runbooks are more than documents—they are sequenced, technically validated guides that spell out restoration priorities, the minimum functionality required for safe care, and manual workarounds that can sustain operations until systems return. They also define service level agreements (such as how quickly critical systems should be restored) and tailor controls and processes accordingly. Importantly, runbooks provide direction, not a script. Each incident is unique, requiring flexible, informed decision making from empowered teams.

Boards also need to see tangible metrics of readiness. For example, how long does it take to restore essential operations during exercises? Numbers alone are not enough, though. Boards should get into the details, too. Which critical systems' recovery procedures have been tested? Have we tested workflows end to end? What vulnerabilities keep resurfacing in downtime drills? Probing at this level helps boards gauge whether plans will hold in practice.

> Boards need to see tangible metrics of readiness to gauge whether plans will hold in practice.

And crucially, each exercise—or when it occurs, each incident—should drive improvement. Simulated or real events should uncover capabilities gaps (that organizations can then prioritize to address), spark follow-through that the board can track, and demonstrate the enhancements made to procedures, contracts, or technology configurations. The goal is a steady rhythm of continuous improvement, ensuring readiness evolves with the threat landscape.

ECOSYSTEM AND DEVICES

Boards should validate how risk is managed beyond their organization's walls. Nearly one in six health care breaches originates with a third party. Organizations rely on an increasingly complex ecosystem, including labs, pharmacies, software vendors, device manufacturers, and revenue cycle platforms. Each vendor exposes the organization to risks that it needs to understand and manage.

Boards can lead by ensuring management applies the same resilience rigor to partners and suppliers that it applies to internal systems. That means conducting tiered, risk-based assessments for vendors that play the most critical roles. For all suppliers, it means implementing contractual expectations around incident reporting and response timelines, as well as continually monitoring vendors' compliance as regulatory scrutiny increases.

Medical devices and Internet of Things systems add another layer of complexity, especially because so many organizations still rely on legacy technology. Boards should look for fundamentals: a complete device inventory, segmentation of high-risk assets to limit the blast radius, vendor-led resilience testing, and clear patching and equipment end-of-life strategies. These controls strengthen the organization's ability to maintain safe, reliable care even when disruptions originate outside its immediate environment.

INVESTMENT AND TRANSPARENCY

Cyber resilience budgets in health care organizations rarely suit the level of exposure, making it crucial for boards to ensure that spending delivers real protection and operational continuity.

Management should explain how each investment improves resilience, whether by reducing downtime, speeding detection and response, strengthening user identity systems and backup capabilities, or addressing emerging risks, such as those introduced by generative and agentic AI.

Investments in talent are equally important. A holistic approach to resilience requires a different skill set than that found in most health care cyber organizations, especially ones at the lower end of the maturity curve. More than ever, organizations need cyber experts with relationship, communications, and business skills—not just tech know-how.

Benchmarking can be especially valuable. Comparing an organization with its peers in the areas of cyber maturity, staffing, and performance can surface blind spots that may otherwise be missed.

Transparency is essential. Boards should ask management to clearly articulate residual risks and tradeoffs, along with evidence of progress: closing security gaps, faster recovery times, stronger maturity scores, or validation from independent assessments. Thoroughness is a virtue here. When conversations focus on outcomes, boards gain a clear line of sight into whether investments mean more resilience—and not simply more funding.

Cyber incidents will happen, but essential care can continue. The most resilient health care organizations design for disruption in advance, building and testing the capabilities that keep mission-critical services stable while the organization recovers.

Focused oversight is pivotal. When boards get it right—when they ask probing questions and hold management accountable for both answers and action—resilience stops being a slogan and starts being a reflex.

Authors

Russell Schaefer

Platinion Managing Director
Washington, DC

Tom Retelewski

Managing Director & Partner
Chicago

Adrian Ciuffetelli

Platinion Director
Philadelphia

Tad Roselund

Senior Advisor
New Jersey

ABOUT BOSTON CONSULTING GROUP

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.