

Five priorities for governing cyber risk in healthcare

Why cyber resilience in healthcare is critical for patient safety.

Digital transformation is reshaping healthcare delivery, creating new opportunities to improve quality, efficiency and accessibility. At the same time, growing reliance on interconnected systems, data and technology providers is making cyber resilience a critical prerequisite for patient safety, operational continuity and public trust. Cyber-security has therefore evolved from a technical function to a board-level responsibility. For healthcare leaders, the challenge is no longer recognizing cyber risk, but ensuring that governance, resilience and preparedness keep pace with increasing digital dependency.

As healthcare organizations continue to expand their digital ecosystems, cyber risk is no longer limited to traditional IT environments. Connected medical devices, cloud services, AI applications and third-party providers are becoming integral components of care delivery. While these developments create significant opportunities for innovation and efficiency, they also introduce new vulnerabilities and dependencies that can directly affect patient safety and business continuity.





A KPMG survey among CIOs at healthcare providers indicates that cybersecurity is widely recognized as an enterprise risk across Swiss healthcare organizations. However, the maturity of cyber capabilities often remains uneven, particularly in areas such as governance, resilience, third-party management and the secure adoption of emerging technologies.

Several key challenges stand out:

1. Governance

Many organizations have incorporated cyber risks into enterprise risk management processes, yet often lack a clearly defined cybersecurity strategy aligned with business objectives. In addition, boards and executives do not always possess the expertise required to effectively oversee cyber-related risks and investments.

Implications:

- Lack of a roadmap towards cyber resilience that is prioritized to enable strategic business objectives
- Limited judgment to challenge current state and way forward of the organization's cyber resilience
- Risk of reactive rather than strategic decision-making

2. Resilience

Operational resilience remains a significant concern. Many healthcare institutions are not confident in their ability to rapidly restore critical operations following a ransomware attack or major cyber incident. Business continuity and recovery plans frequently remain insufficiently tested.

Implications:

- Potential impact on patient safety and operational continuity in case of a cyber incident

3. Third-party dependencies

The increasing reliance on cloud providers, technology vendors and digital supply chains expands the healthcare cyber risk landscape. As critical services increasingly depend on external partners, resilience can no longer be viewed solely from an internal perspective.

Implications:

- Insufficient transparency and understanding of their own cyber risk exposure
- Insufficient ability to respond to cyber incidents involving third parties

4. Medical technology and OT

The growing connectivity of medical devices and operational technology environments creates additional security challenges. Many institutions still lack complete visibility into connected assets, despite their importance for clinical operations and patient safety.

Implications:

- Expanded attack surface through connected, often less secured devices
- Need for specialized expertise to secure OT environments

5. Artificial intelligence

AI presents considerable opportunities for innovation and efficiency but also enables more sophisticated attack methods. Organizations increasingly face risks related to impersonation attacks using deepfakes, automated phishing campaigns, and AI-assisted cyberattacks.

Implications:

- Faster cyber incident response capabilities are required
- Robustness of digital identities is critical
- Traditional ways to manage system vulnerabilities are no longer sufficient to handle AI-assisted cyberattacks

Against this backdrop, cybersecurity should be viewed as a strategic capability and not a standalone security function. Organizations that successfully combine strong governance, operational resilience, third-party oversight and secure technology adoption will be better positioned to realize the benefits of digital transformation while maintaining trust among patients, regulators and other stakeholders.





“Cybersecurity should be viewed as a strategic capability and not a standalone security function.”

Key actions for healthcare organizations

The board should oversee and challenge the executive team in the following areas:

Cybersecurity must become a strategic leadership priority

Healthcare organizations should establish a clear cybersecurity strategy, ensure access to cyber expertise at board level, and challenge the executive team to align the cyber roadmap with business objectives and priorities. This should be supported by cross-sector collaboration, for example with the recently established Healthcare Cyber Security Center (H-CSC), which enables them to proactively manage cyber risks, reinforce resilience and maintain trust among patients and the public.

Systematically build resilience

Resilience depends on a good understanding of dependencies, regularly tested recovery capabilities, and stronger crisis management and incident response processes. In addition, robust identity and access controls, and continuous improvements in vulnerability management are required to keep pace with increasingly sophisticated AI-enabled threats.

Actively manage third parties and supply chains

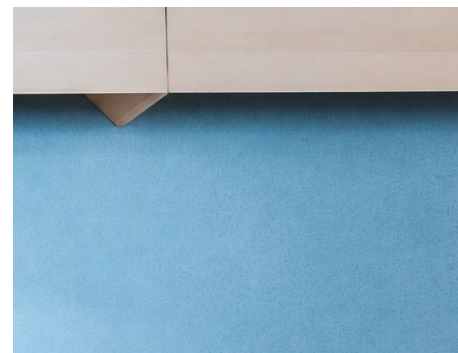
Effective third-party risk management starts with identifying and prioritizing critical suppliers, embedding cybersecurity requirements into procurement and contracts, and continuously assessing and monitoring external risks across the broader digital ecosystem.

Ensure transparency in connected medical technology

A comprehensive inventory of medical devices provides the foundation for identifying critical systems and dependencies and fully integrating medical technology into cybersecurity, crisis management and recovery planning.

Safely deploy and scale AI and new technologies

Clear governance structures for AI and cloud applications, combined with security requirements embedded in digitalization and AI projects, support the safe deployment and scaling of new technologies.





Conclusion

Cyber resilience is a strategic imperative for healthcare organizations as increasing digitalization, interconnected systems and emerging technologies create both new opportunities and greater cyber risk. To protect patient

safety, operational continuity and public trust, boards and executive teams must align cybersecurity with organizational strategy, strengthen resilience capabilities, actively manage third-party dependencies, secure connected medical technologies and govern the adoption of AI and other emerging technologies.

Authors



Matthias Bossardt
Partner,
Head Risk Consulting Services
KPMG Switzerland

mbossardt@kpmg.com



Gabriela Kern
Director,
Government & Healthcare
KPMG Switzerland

gkern@kpmg.com

This article is part of KPMG's Board Leadership News.

About the KPMG Board Leadership Center

The KPMG Board Leadership Center offers support and guidance to board members. We equip you with the tools and insights you need to be highly effective in your role, enabling you to focus on the issues that really matter to you and your business. In addition, we help you to connect with peers and exchange experiences.

Learn more at kpmg.ch/blc

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received, or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. The scope of any potential collaboration with audit clients is defined by regulatory requirements governing auditor independence. If you would like to know more about how KPMG AG processes personal data, please read our **Privacy Policy**, which you can find on our homepage at www.kpmg.ch.

© 2026 KPMG AG, a Swiss corporation, is a group company of KPMG Holding LLP, which is a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.