Cybersecurity in Health Care

Educational Briefing for Non-IT Executives

Executive Summary

Health care organisations (HCOs) historically have dedicated limited time and resources to cybersecurity often seeing it simply as a compliance issue. That's changing, in light of the many significant recent cyber events across industries. Yet, key leaders still often don't have a clear path to engage in security matters. Senior leadership across all organisational functions, including the CEO and board, are accountable for mitigating the organisation's cyber risk and thus have a critical responsibility: enable, support, and promote cyber resiliency within their organisation. True cyber resiliency—the ability to predict, prevent, address, recover, and learn from cyber incidents—extends beyond technical controls and is built holistically through effective governance and policy, process and education, as well as technology and services. This wider perspective brings to light several critical areas within which senior leaders can make a significant impact.

What is cybersecurity?

Cybersecurity refers to the set of techniques organisations use to protect their information systems, networks, devices, and confidential data against attack, damage, or unauthorised access. These techniques include technologies and processes such as data encryption, identity management and access control, threat intelligence, disaster recovery, and staff security awareness training and testing, among many others. Cyber threats come in many forms and cyber criminals use a variety of attack vectors to gain access. In the past, lost or stolen devices and insider abuse were top concerns, but while these internal threats remain, external threats such as phishing and probing attacks have surged. Below is a graphical depiction and brief explanation of several common threat vectors.

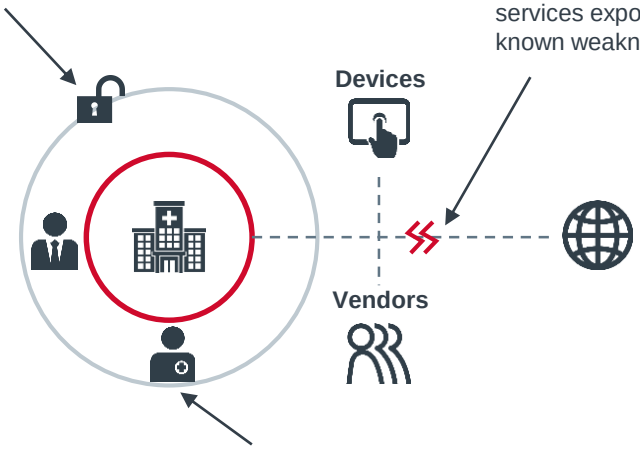
Prevailing Cyber Threat Definitions

Social Engineering: A broad threat category in which the perpetrator uses various means to persuade the victim into performing actions or divulging information for malicious purposes.

Phishing: Form of social engineering that generally uses email as a vehicle for perpetrating the act.

Spear Phishing: Form of phishing in which the victim is specifically targeted.

Whaling: Form of spear phishing in which the targeted individual is someone of significant importance or access to funds within the organisation such as a CEO or CFO.



Probing: A threat vector in which the perpetrator scans devices and services exposed to the internet for known weaknesses.

Insider Abuse: Broadly, a threat vector in which the attack comes from inside the firewall. The category includes both deliberate actions as well as vulnerabilities unintentionally introduced into the network by authorised third parties.

Why is it important?

First and foremost, cyberattacks compromise patient privacy and potentially patient safety. The entire enterprise is at risk, not just IT. Major, disruptive attacks may prevent providers from caring for patients, HCOs may lose access to or have patient records completely deleted, and expensive diagnostic equipment and other medical devices may be rendered unusable. There are also large financial implications at stake due to the cost of clean up and recovery efforts, significant fines and settlements, legal settlements, and class action lawsuits, which can all amount to multi-millions in cost.

Source: Advisory Board interviews and analysis.

How is cybersecurity addressed in health care?

While critically important, technology alone is insufficient to mitigate cyber risk. Cyber resilience requires an ecosystem of efforts in three crucial areas: governance and policy, process and education, and technology and services.

Governance and Policy

- C-Suite and Board Engagement
- Dashboards
- Governance
- Standards
- Strategy
- Digital Trading Partners
- Staffing

Process and Education

- Training/Testing
- Incident Response Planning
- Risk Assessments
- Audits
- Business Continuity Planning, Back-ups, and Disaster Recovery

Technology and Services

- Cyber Intelligence
- IT-Enabled Capabilities
- Cyber Insurance
- Information Sharing

How does cybersecurity affect health care providers and IT leaders?

Today's HCOs must build cyber resilience across the enterprise and dedicate attention to all three ecosystem layers described above. To get started, we recommend HCOs:

- **Grow sophistication over time:** Ensure the basics are in place. Understand your current state and address any gaps in all critical areas. Advance security maturity over time ensuring efforts match the HCO's culture, operations, and acceptable risk level.
- **Forge and maintain partnerships between IT and non-IT leaders:** Strong, effective partnerships between IT and security leaders with individuals inside and outside of the C-suite and boardroom are essential.
- **Understand and address third party risk:** Recognise that your business partners—including vendors and M&A[1] activity—broaden your organisation's cyber risk. Include security as a vital component of due diligence; actively manage cyber risk throughout any relationship; and consider a set of minimum standards for doing business.
- **Promote a security-focused culture:** Executive leadership must show support for all components of the cybersecurity ecosystem, treat security as a team sport, not place blame when something inevitably happens, and hold all staff accountable for protecting the organisation.

Questions That Hospital Executives Should Ask Themselves

1. Do each of the organisation's senior leaders understand the role they play to protect the organisation?
2. Have you established a clear objective for cybersecurity risk? Do you have a security strategy?
3. Does the security governance structure provide end users a voice in decisions impacting their work?

Additional Advisory Board research and support available

Infographic: Paint a Picture of a Cyber-Resilient Organisation

Infographic: When a Cyberattack Occurs, the Whole Hospital is Our Patient

On-demand Web Conference: How to Build a Breach Plan

1) M&A = Mergers and acquisitions.

Source: Advisory Board interviews and analysis.