4 Steps to Creating a Culture of Cybersecurity in Healthcare

The father of corporate leadership, Peter Drucker, said that "culture eats strategy for breakfast" meaning that an organization's culture is not only stronger than any single strategy, it determines the ultimate success of the enterprise. Regardless of an organization's cybersecurity strategy or program, if employees don't embrace it as part of the culture, the odds of success are very low.

Culture reflects not only the "real" values of the organization, but the behaviors and actions employees take when responding to everyday challenges or critical events–It's what they do when no one is looking. An organization's ability to execute on its cybersecurity strategy hinges on its employees' understanding, acceptance, and disposition to the vision, tasks, and expected results of the strategy.

Here are 4 critical steps for healthcare leaders to consider when building a culture of cybersecurity based on meaningful cyber risk strategies and decisions:

1. Make Patient Safety a Core Pillar of Cyber Strategy

Regardless of size, healthcare delivery organizations (HDOs) share a common mission to improve the health and lives of patients in accord with a set of immutable values: respect, compassion, community, and care experience. Given the reliance on technology and the associated cyber threats which come along with its usage, the connection between patient safety and cybersecurity is more critical than ever. In the same way hand-washing was once connected to infection rates, hospitals may consider leveraging internal communications to emphasize the importance of cybersecurity with "Cyber Safety is Patient Safety" or "Ransomware Risks Patient Care" posters.

When an HDO elevates the protection of patient care against cyber threats to one of its core values, it emboldens employee culture and draws a critical 'line in the sand': we protect patient safety at all costs regardless of the source of threat (e.g. medical, technical, internal threat, nation state cyber attack).

2. Align Cybersecurity Accountability at the Top

Cybersecurity risk is a top three critical business issue facing the HDO board of directors today. Unfortunately, most board members are not technology experts, and IT leaders often struggle with communicating cybersecurity risk in a way that aligns with business objectives. These leaders must work together to understand the dependencies of digital data and technology across all clinical and business processes.

Cyberattacks threaten all electronic healthcare data and systems. Therefore, cybersecurity risks must be managed across all HDO operations and supporting systems including:

- Daily Operations: email, patient scheduling and administration, accounting and financials.
- Clinical Operations: EMR, labs, radiology and discharge.
- Third Parties: critical vendors and products.
- Supply Chain: medical supplies, pharmacy, PPE, laundry services and HVAC.
- Innovation/Research: drug discovery, wearables, telehealth, internally-developed applications, and the institutional review board.
- Joint Venture/M&A: acquisitions, affiliated practices & sites, and special projects.

An integrated approach to cyber and enterprise risk builds a culture of coordination, collaboration and communication in a trusted way.

Targeted, dedicated Board-level discussions about cybersecurity –and critical existing gaps in security–help the directors consider appropriate trade-offs between business objectives and risks, and assures sufficient staffing resources, training, tools and investments are made to reduce risks across the enterprise. Boards should consider adding a dedicated operating committee for cybersecurity. As top-down accountability for cybersecurity permeates the organization, the culture will take notice and respond in kind.

3. Elevate and Transform Cyber Risk as Enterprise Risk

Once values and leadership are aligned, the next step is to empower the culture to transform how it manages cyber risks. First, stop treating cyber risk as "an I.T. issue" and elevate it in the broader context of mission and business objectives. This establishes a baseline for overall governance with alignment of business objectives against cybersecurity risks to patient safety, care delivery, business operations, data, and reputation.

By managing cyber risk as enterprise risk, a common framework, language, and reporting approach are established among operational and leadership teams. Additionally, cybersecurity and enterprise risk practitioners can drive meaningful discussions on gaps, requirements, and priorities that establishes cybersecurity risk as an important element of effective enterprise risk management.

Boards can help mitigate cyber risks and damages by actively measuring progress governing the effectiveness of the overall cybersecurity program. The leadership team can consistently frame cybersecurity risks and controls in a language that the board understands and can use to challenge assumptions, provide guidance and oversight, and help make meaningful risk decisions.

4. Engage and Empower Employees Frequently on Cybersecurity

The last step to successfully creating a culture of cybersecurity in healthcare is to build a program of proactive and frequent employee engagement. Survey a portion or all of your employees to establish a baseline of cyber knowledge. Establish an employee-led task group to help identify gaps in training and internal communication processes, develop an employee-led vision for the cyber program, and encourage input into a formal cybersecurity engagement program.

Regular virtual and on-site training ensures all employees understand the importance of cybersecurity, their role and expected behaviors, and how their work contributes to protecting patient safety and the core mission. Compliment training and strengthen a culture's "muscle-memory" and impact by rewarding employees and celebrating cyber wins formally during a town hall meeting and/or virtually in a dedicated Slack or Microsoft Teams channel. Consider holding retrospective sessions as needed to learn from mistakes or actual incidents.

An organization with a strong vision, defined values and reward system, and clear employee expectations has a high chance of nurturing and developing a culture of cybersecurity and patient safety.

Final Thoughts

Studies show that cultures which fuel its employees' passion for mission and goals consistently deliver on their strategies and meet objectives over time. Building a strong culture of cyber protection and patient safety requires consistent reinforcement of why short-term wins matter and how they lead to the achievement of a long-term vision that benefits everyone in the organization. Cyber strategy is crucial for setting direction and focus. Cyber strategy focuses on resources, investments, policies, procedures, skills, tactics, tools, and processes, but it is a strong cyber culture that guarantees engagement and execution, and ultimately determines whether a strategy lives or dies.

If you would like to learn more, contact us at info@censinet.com or visit https://www.censinet.com

KLAS RESEARCH CENSINET MEASURED Cybersecurity Transparent

American Hospital Association Preferred Cybersecurity Service

CHIME

Censinet is an American Hospital Association Preferred Cybersecurity Service Provider for Cyber Firm Risk Management and Information Governance and Cyber Risk Assessment, Privacy and HIPAA Compliance.