5 Best Practices for Reducing Enterprise Cyber Risk

As ransomware continues to threaten care operations at hospitals and health systems across the country, managing enterprise cyber risk now means managing risks to patient safety. This Solution Brief provides 5 best practices for identifying, managing, and mitigating enterprise cyber risk to help health systems strengthen cyber resiliency and protect patient safety from these malicious threats:

1. Develop a Clinical Continuity Plan

As ransomware attacks on U.S. hospitals intensify in magnitude and malignity, healthcare leaders must ensure they have continuity plans for both business and clinical functions in the event of protracted downtime. While a business continuity plan is typically owned by IT, a clinical continuity plan is created by an interdisciplinary team and codifies downtime procedures for all network-connected, mission-critical systems involved in care delivery. For example, per a recent alert released by The Joint Commission, a clinical continuity plan may include "contingency plans on how to treat stroke, trauma, and heart attack patients without the availability of normal imaging technology and catheterization labs – or how to continue delivering radiation oncology and chemotherapy."

In addition, effective clinical continuity plans prepare for the broader regional impact of ransomware attacks. A recent JAMA study found that a ransomware attack at a single healthcare delivery organization (HDO) can have a substantial impact on care delivery at multiple nearby hospitals. The study concludes that hospitals adjacent to an HDO undergoing a ransomware attack "may see increases in patient census and may experience resource constraints affecting time-sensitive care for conditions such as acute stroke" as emergency rooms shut down, ambulances are diverted, and tests/procedures are canceled.

2. Adopt Recognized Security Practices

"Recognized security practices" like NIST Cybersecurity Framework (NIST CSF) and 405(d) Health Industry Cybersecurity Practices (HICP) are industry-approved best practices and frameworks for improving cybersecurity maturity and resiliency. By law, HHS Office for Civil Rights (OCR) is required to take recognized security practices into consideration when determining remedies for violations of the HIPAA Security Rule. While not Safe Harbor, if covered entities and business associates can demonstrate 12 months of coverage for NIST CSF or HICP to the OCR, it may result in reduced fines, penalties, or an early, favorable termination of audit.

NIST CSF enables healthcare leaders to measure the organization's overall ability to Identify, Protect, Detect, Respond, and Recover from cybersecurity risks and threats. Automating enterprise assessments and action plans for NIST CSF Categories and Subcategories helps prioritize resource allocation and investment decisions. HICP identifies the top five cyber threats and provides ten best practice areas that can be used to mitigate these threats. These best practices are based on NIST CSF, vetted by healthcare and security professionals, and can drive immediate improvement in an organization's cyber hygiene.

3. Benchmark Against Peers

Peer benchmarking is one of the most effective ways to drive continuous improvement and maximize cybersecurity investment. Best practices for cyber peer benchmarking include:

- Comprehensive benchmarks across recognized security practices – NIST CSF and HICP – as well as key cost, productivity, and program ownership metrics
- Highly-precise peer group comparison and filtering driven by a robust sample size across multiple types of healthcare organizations
- Automated enterprise self-assessments and action plans for NIST CSF and HICP to identify and close critical gaps in controls
- Intuitive dashboards to communicate relative performance and justify targeted investment with the Board

Leading organizations deploy peer benchmarking across all parts of the health system – from hospital to clinic to practice – to ensure the entire enterprise keeps pace with peer and industry performance.

4. Assess All Third-Parties

Half of all healthcare breaches are caused by third-party vendors; yet, quite often, health systems suffer the majority of the fallout. Despite best intentions, resource constraints and antiquated tools prevent most organizations from performing risk assessments (and reassessments) across all third-party vendors, products, medical devices, and non-technical suppliers. Best practices for more efficient, effective third-party risk management (TPRM) include:

- Get full risk visibility by creating a centralized, digital inventory of all third-parties
- Tier third-parties based on business impact (e.g. Critical, High, Medium, Low)
- Adjust product risk profile based on business use case and your IT environment
- Automate corrective action plans (CAPs) and remediation tracking & assignment
- Schedule reassessments based on risk tier and use AI to show what's changed since last assessment

Using these best practices, leading organizations can significantly speed up the TPRM process, and begin to assess, reassess, and reduce risk across all of their third parties.

5. Leverage the Entire Enterprise

Leading organizations enfranchise and engage all stakeholders across the enterprise to reduce cybersecurity risk. Key tactics include:

- Integrating third-party risk assessments into workflow ticketing systems
- Working with business owners to manage a centralized risk register
- Assigning corrective action plan items to internal subject matter experts
- Automatically linking vendor remediations to Legal / contracting teams
- Reporting to the Board with an intuitive, non-technical, and consistent risk framework

Final Thoughts

As ransomware continues to proliferate, fighting back against the bad actors who threaten patient care begins with these five best practices for faster, more effective enterprise cyber risk management. If you would like to learn more about third-party and enterprise risk management, please contact us at info@censinet.com. Censinet is an American Hospital Association Preferred Cybersecurity Service Provider.

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

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.