Measuring What Matters for Cybersecurity in Healthcare

Patient safety and care disruption are now in the cross-hairs of cyber attackers, leaving many healthcare leaders to wonder whether their organizations are truly prepared when an incident occurs. Healthcare leaders must be able to actively track, measure, adjust, and improve progress and effectiveness of their cybersecurity program.

Consider the following three steps to identify, manage and measure progress and effectiveness of a healthcare delivery organization's (HDO) cybersecurity program:

1. Measure What Matters

> *"Not everything that can be counted counts, and not everything that counts can be counted."*
>
> - Albert Einstein

The hardest thing about managing a cybersecurity program is measuring the results. How quickly can we identify, respond to, and recover from a cyber attack? What's the impact of an attack on patient care? What is the full cost of an incident?

When measuring cybersecurity, it's important to know whether or not there's been an incident in the last 12 months and how quickly the response and recovery were for the incident. Measuring the mean time for response and recovery is an effective way to measure how quickly the HDO can recover from an attack. Equally important is understanding the frequency of incidents, or Mean Time Between Incident (MTBI) as a way to measure cybersecurity program effectiveness over time.

Using a MTBI metric assumes that it's not a matter of if but when a cybersecurity attack and incident will occur and focuses on continual improvement of the program. MTBI indicates the duration that business operates without cybersecurity disturbances or outages. This intuitively relates to the availability of digital assets that support critical operations such as care delivery, biomed, radiology, and revenue cycle.

The availability or uptime of a hospital can be a key indicator of overall operational effectiveness and an excellent way to identify areas of potential cybersecurity program gaps and overall productivity improvement. A healthcare organization's total uptime therefore can be expressed in terms of the MTBI together with another metric, the MTTR (Mean Time To Recovery).

2. Use Recognized Cybersecurity Frameworks and Practices

> *"If you can't measure it, you can't improve it."*
>
> - Peter Drucker

Compliance to and/or coverage of recognized industry security practices such as NIST Cybersecurity Framework (CSF) or HHS 405d Health Industry Cybersecurity Practices (HICP) is a good approach to measuring cybersecurity program health and maturity. To reduce the occurrence and impact of an incident, HDO leaders may consider actively measuring and trending the progress and effectiveness of their overall cybersecurity program using these practices.

The NIST CSF enables healthcare leaders to measure the healthcare organization's overall ability to identify, protect, detect, respond, and recover from cybersecurity risks and threats. Assessing and analyzing the risk across these five categories helps the organization measure the likelihood and impact of a cybersecurity event. Further measurement and analysis of the CSF subcategories aids in determining gaps and a prioritized action and investment plan to address those gaps. An organization's compliance to the NIST CSF and coverage of implemented security controls can be regularly assessed and measured to continuously improve the effectiveness of its overall cybersecurity program.

As a result of the Cybersecurity Act of 2015, the U.S. Department of Health and Human Services (HHS) convened a public-private working group to develop and publish the Health Industry Cybersecurity Practices (HICP). The HICP publication identifies five current cybersecurity threats and provides ten practices that can be used to mitigate them. These best practices are based on the NIST CSF and vetted by healthcare and security professionals.

Recognized security practices such as NIST CSF and HICP provide not only a sound foundation for cybersecurity program measurement but they also can be used to document and prove an HDO's ability to meet the "duty of care" for protecting patient data. Section 13412 of the HITECH Act requires HHS to take into consideration certain recognized security practices of covered entities and business associates when determining potential fines, audit results, or other remedies for resolving potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule pursuant to an investigation, compliance review, or audit. Public Law 116-321 went into effect when it was signed into law on January 5, 2021.

3. Leverage Peer Benchmarking Whenever Possible

> *"One measurement is worth a thousand expert opinions."*
>
> - Donald Sutherland

Peer benchmarking is an approach for comparing the overall strategy, design, implementation, resources, and effectiveness of one organization's cybersecurity program against that of another organization. This process can be used to compare best practices, performance metrics, tools, processes, people, ownership, coverage and other metrics to help learn how well one HDO performs over a cohort of similar HDOs based on location, size, or model.

The ability to compare organizational and cybersecurity metrics across a peer group is commonly sought after by most healthcare CIOs/CISOs. Applying organizational and investment benchmarks helps answer the question that every healthcare Board member will ask: How do we compare with our peers? The overall industry? Where are the gaps in coverage, people, skills and education? Where do we need to invest and why? What happens if we do nothing?

Benchmarks provide healthcare leaders with the ability to measure cybersecurity performance in the context of the larger industry and against peers, enabling more informed, data-driven decision making. Peer benchmarks may also reflect a larger shift in the overall healthcare market as it relates to cybersecurity. For example, a less mature HDO may only be focused on a cyber risk within IT while its peers may be measuring cybersecurity risks across all of its business processes, 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.

Final Thoughts

The effectiveness of a healthcare organization's cybersecurity program is directly related to its ability to measure business objectives, investments, and specific outcomes. Whether it's the performance of people, process, or technology, improvements cannot be made if they cannot be measured. To get the most out of a cybersecurity program, healthcare leaders must consider using industry recognized security practices and peer benchmarks to measure what matters most. AHA Cybersecurity Preferred Solution Providers such as Censinet offer integrated risk management solutions that measure cybersecurity program effectiveness based on recognized security practices and peer benchmarks.

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.