




Maximize Cybersecurity Investment and Performance with Peer Benchmarking



Over the last two decades, healthcare has spent billions to transform from paper-based care to electronic health records, and billions more have been spent on creating a full digital care delivery system. With this shift has come extraordinary gains in clinical performance, but also substantial increases in cyber risk. And despite heroic efforts by healthcare delivery organizations (HDOs) to keep pace, the inexorable confluence of an ever-evolving threat landscape and an ever-expanding attack surface seem to keep us always one step behind.

With billions of dollars now poised to be spent on cybersecurity across the next decade, CIOs and CISOs are asking:

- 1. Where do I prioritize investment to maximize the long-term maturity, strength, and resilience of our cybersecurity program?*
- 2. Where should I allocate scarce resources to immediately elevate our cybersecurity program's performance and productivity?*

Cyber peer benchmarking can help you make more informed, data-driven decisions to answer these critical questions.

1. The Value of Cyber Peer Benchmarking

As HDOs scramble to stay ahead of bad actors, CIOs and CISOs are asking all the right questions, but are often left with insufficient answers:

- Are we adequately protecting patients from cyber risk?
- How mature is our cybersecurity program?
- Do we follow industry recognized security practices?
- Where do we have critical security gaps?
- How does our security program performance compare to peers?
- Where should we prioritize cyber investment and allocate resources?
- How do I successfully communicate and justify requests for capital?

Benchmarking provides objective, actionable answers to these questions and drives data-driven decision-making across cybersecurity program strategy and operations:

Prioritize and Justify Cybersecurity Investment – See how your cybersecurity investments compare to peers at any given point in time and identify where your organization lags or leads similar organizations across key categories. Use benchmarking results to help prioritize future investment decisions and justify capital requests to the Board.

Elevate Cybersecurity Program Performance – Compare your cybersecurity program's performance to peers across key productivity and cost metrics. Use benchmarking results to identify where your organization lags peer organizations and justify increased budget to keep pace.

2. Benchmark Across a Diverse Set of Cyber Risk Categories

Benchmarking begins with an objective self-assessment of your cybersecurity program across a diverse set of industry recognized security practices and key performance indicators, including:

NIST Cybersecurity Framework (NIST CSF)

The U.S. government-based NIST CSF enables HDOs to measure, manage, and improve an organization's ability to Identify, Protect, Detect, Respond, and Recover from cyber threats and security incidents. Building your cybersecurity program's foundation on top of NIST CSF helps to ensure comprehensive, continuous improvement in program maturity. Self assessment and peer comparison against NIST CSF's 5 Functions, 23 Categories, and 108 Subcategories provides a detailed, comprehensive lens on security program maturity; and, as such, delivers a more targeted and tactical action plan for future investment.

Health Industry Cybersecurity Practices (HICP)

As part of the Cybersecurity Act of 2015, HHS convened a public-private working group to publish the 405(d) Health Industry Cybersecurity Practices (HICP), which identifies the five most common cybersecurity threats and the ten best practice areas that can be used to mitigate these threats. These best practices are based on the NIST CSF and are curated by healthcare cybersecurity professionals. For security programs that don't yet have the time and resources to implement NIST CSF, HICP is a relatively a more manageable starting point that still provides a strong, healthcare-specific security framework to improve cyber hygiene.



Organizational Cyber Performance

Measuring and comparing key performance indicators provides actionable insight into how your organization's day-to-day cyber operations lags or leads peer organizations.

Peer comparison across a diverse set of productivity, cost, and performance indicators ensures comprehensive evaluation of current security program performance and points a direct path to improvement.

Key Organizational Cyber Metrics Include:

- % Cyber Expense to Revenue
- % Cyber Expense to IT Expense
- % IT Expense to Revenue
- % Program FTE Ownership
- Employee to Cyber FTE Ratio
- Cost to Protect each Workforce Member
- Cost to Protect Patient Record
- Cyber Insurance Premium Increase



3. Closing the Gap with Peer Benchmarking Automation

With a significant amount of data to manage, leading organizations are fully automating the peer benchmarking process. Key capabilities and benefits of these automated peer benchmarking platforms include:



Standardized, Curated Questionnaires for Apples-to-Apples Comparison

Out-of-the-box, standardized questionnaires – curated to industry recognized security practices for healthcare – ensures an apples-to-apples comparison of your organization against peers. Continuous curation targets the unique and ever-changing risks faced by healthcare organizations and ensures security frameworks remain up-to-date.



Automated Action Plan Generation for Targeted, Continuous Improvement

Action plans with recommended remediations are automatically generated and tracked to ensure efficient, effective, and continuous improvement of your own organization's cybersecurity performance; while, at the same time, helping to close the gap against peers.



Built-In Evidence Capture for Validated, Trusted Benchmarks

Prompting users to provide documentation and evidence enables security leaders to validate responses, update legacy policies, and easily maintain a centralized, longitudinal risk record. What's more, this 'single source of truth' for each organization across the peer group ensures accurate, up-to-date, and objective benchmarks you can trust.



Risk Ratings & Reporting for a Real-Time, Intuitive Lens on Cyber Performance

Auto-generated risk ratings and summary reporting enables security leaders to communicate real-time enterprise risk posture to the Board. Backed by benchmarking results, CIOs and CISOs can objectively demonstrate where the organization's cybersecurity program lags their peer group and then justify investment based on empirical data.

Final Thoughts

Like a rising tide, peer benchmarking not only helps to set a future course for one's own cybersecurity program, but charts a collaborative trajectory for the industry as a whole, making all healthcare organizations more secure, resilient, and stronger together. If you would like to learn more, contact us at info@censinet.com or visit 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.