A Solution Buyer's Guide to Cyber Risk Management

Healthcare delivery organizations (HDOs) have many options to consider when seeking to improve their cybersecurity risk management programs. From spreadsheets to certifications, managed services to risk ratings, and GRC to risk exchanges, all of these solutions can bring significant benefits to cyber risk management, driving insight and improvement across an organization's third party and enterprise risk management functions.

Learn about each category of solution available, the key trade-offs and considerations of each option, and best practice evaluation criteria for these cyber risk management solutions:

Internal Applications

This category of solutions generally includes a constellation of legacy tools such as spreadsheets, word processing, and slide presentations – with email serving as the backbone of communication internally and between HDO's and their third-party vendors.

Key Considerations

- While these tools are readily available, familiar, and fit within budget, the risk workflows inside these applications are often labor intensive, time-consuming, and heavily manual.
- These tools offer little automation or economies of scale for budget-constrained teams seeking to expand the reach of their cyber risk management program.
- HDO's seeking to increase risk coverage of all third parties across the full vendor and product lifecycle – purchase, implementation, integration, usage, updates, renewal, retirement – often struggle to find leverage and scale with these solutions, and, as such, often fail to keep up with an ever-increasing amount of risk debt.

Best Practices for Evaluation

- In light of the current threat landscape and economic environment, most HDO's will have to do more with less, so most will find these legacy solutions inadequate to meet their needs.
- Moreover, with rising mandates to protect patient safety from sophisticated threats like ransomware, leading HDO's are retiring use of these legacy tools and actively migrating to automated solutions for increased scale, leverage, and effectiveness.

Frameworks, Security Practices, and Certifications

This category includes everything from for-profit companies to not-for-profit certifications to government-based cybersecurity frameworks. Many organizations find this category difficult to navigate, with a dizzying array of certifications, attestations, badges, frameworks, best practices, industry standards, and "de facto standards."

Key Considerations

- Many options in this category are not optional; as such, the first step for buyers is to work with their Legal & Compliance teams to determine which controls, policies, and procedures are mandatory for a given entity type, IT environment, or application (e.g., covered entity, business associate, medical devices, clinical/cloud applications).
- The key trade-off for optional certifications is: time and money spent vs. realized benefit and efficacy to cybersecurity program maturity, strength, and resilience.
- For HDOs, recognized security practices such as NIST CSF or the HHS 405d Health Industry Cybersecurity Practices (HICP) are free to implement, and, under Public Law 116-321, may provide relief from regulatory enforcement upon a security incident.

Best Practices for Evaluation

- Frameworks and Practices are best implemented with automated capabilities like continuous monitoring, automated remediations, trending and reporting, and peer benchmarking.
- While Certifications often bring external validation to cybersecurity programs, most are very costly, time-consuming, and only point-in-time – resulting in decreased effectiveness and accuracy by the time they are completed and published.

At the end of the day, many of the certifications and frameworks in this solution category are based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), a U.S. government-based framework for all industries, and the current "gold standard" for cybersecurity controls, policies, and procedures. As such, leading healthcare CIOs and CISOs use NIST CSF as the core foundation of their security programs, with many leveraging automation to assess their organization's adoption and compare coverage to peers.

> *"We chose Censinet because of its simplicity, productivity, and the opportunity to join their risk network, which provides a unique approach to managing third-party risk. Censinet will enable us to streamline our assessment workflows, substantially reduce assessment completion time, and allow us to respond more quickly to potential threats."*
>
> — James Case, Vice President and Chief Information Security Officer at Baptist Health

Risk Ratings

Security risk ratings companies generally take an "outside in" approach to measuring organizational risk posture – running sophisticated algorithms to find potential vulnerabilities and security gaps within an HDO and its third-party vendors and suppliers, or find stolen credentials or other data on the dark web such as protected health information (PHI).

Key Considerations

- Many solutions in this space provide a detailed, comprehensive view of a vendor's external risk posture and most HDOs use these systems to conduct regular security scanning of their third-party vendors.
- These solutions only scan what they can "see"; consequently, for third party risk, they provide risk scoring only on the vendor organization, not on the vendor's myriad products used by an HDO.
- Reducing cyber risk down to a single score, CIOs and CISOs should consider what data is necessary and available vs. what is sufficient and needed to conduct effective cyber risk assessments.

Best Practices for Evaluation

- There is generally no visibility into third party controls, policies, and procedures. As such, look for automation that combines vendor and product assessment capabilities with the "outside in" approach.

Managed Services Providers (MSPs)

Managed services providers offer a wide variety of services to HDOs via a platform that they own or through a partner, including turn-key vendor risk management, IT implementation, MSSP/SOC services, and security consulting.

Key Considerations

- Within vendor risk management, MSPs are generally a good option for those who want to completely outsource their third party risk assessment activities, or for those that lack the resources to bring that function completely in-house.
- Offering a "one-stop shopping" value proposition, HDOs can expect to receive regular reporting on risk posture from their MSP as well as customized consulting and implementation services – at additional cost – for identified security gaps and IT infrastructure needs.

Managed Services Providers (MSPs) continued

Best Practices for Evaluation

- Research and trust is critical in this space, as core risk management functions are often fully offloaded to the MSP; moreover, some MSPs use extensive offshore resources to keep pricing competitive, which may introduce additional risk exposure and data governance concerns.
- During evaluation, technical maturity should be considered as well – *how* an HDO's risk data is processed is just as important as where and by whom. MSPs using rote methods and antiquated technologies may not adequately capture all the dimensions and drivers of cyber risk. So despite best intentions, MSPs may not be able to quickly and effectively respond to, and recover from, a security incident.

Like all solutions, you get what you pay for, and this applies to MSPs. Given the increasing sophistication of ransomware, HDOs should consider leveraging managed services that provide long-term options (i.e. full, hybrid, platform) that future-proof their risk programs.

Tech-Enabled Services

A sub-category within Managed Services (or an extension thereof), these solutions are typically built in support of an existing services business. They use varying degrees of custom-developed automation, storage, and workflow to facilitate the delivery of these services.

Key Considerations

- For cyber risk management, these solutions generally offer a more narrow scope of services compared to MSPs (as described above).

Best Practices for Evaluation

- Buyers here should seek to distinguish between real differences in value creation versus just marketing-speak. Look behind the curtain at the technology enabling the service and what happens with your cyber risk data.
- Ask critical questions, like: What is the technology being used (e.g., Microsoft SharePoint, custom-developed web portal, desktop application, etc.)? Does the service solely benefit the solution provider? What are the data use policies during and post-engagement? Who is doing the work and where is the work done physically?
- Purported technical advantages (and the promised gains passed through to the customer) can vary substantially; moreover, if HDOs are paying a premium for these solutions, careful consideration should be given to long-term leverage of the data and overall insight.

GRC Platforms

Governance, Risk, and Compliance (GRC) platforms offer a broad solution across the healthcare organization to manage multiple functions, ensure accountability and compliance, and centralize myriad risk management processes, including third-party and enterprise risk.

Key Considerations

- While GRC platforms promise to deliver an all-in-one solution to support an organization's risk function, results to date are mixed and undesirable trade-offs persist.
- Current GRC platforms in healthcare tend to offer significant breadth, but often deliver little depth in terms of features, functionality, and capabilities to automate the cyber risk management activities that drive real efficiencies and effective outcomes.
- While many GRC platforms tout their flexibility and customizable features, many users report that too much flexibility and customization can make it difficult and time consuming to configure, implement, manage, and maintain.
- Moreover, many GRC platforms require dedicated and costly development, configuration, and administration support. Unfortunately, these services can often cost more than the application license itself over time.

Best Practices for Evaluation

- No purpose-built GRC platform for healthcare exists, so buyers must evaluate solutions built for other industries that have been "re-purposed" for healthcare; as such, the amount of healthcare-specific curation and risk capabilities should be carefully evaluated and researched.

Healthcare Purpose-Built Risk Exchanges

A new, emerging class of solutions such as Censinet RiskOps™ are purpose-built risk exchanges that enable streamlined risk workflow automation, continuous monitoring of risk, and secure, dynamic information sharing of data and risk insight between HDOs, their peers, and the supporting ecosystem of partners, third-party vendors, and products.

Key Considerations

- Purpose-built risk exchanges focus on fully automating all existing healthcare risk workflows, enabling HDOs to manage and mitigate third party risk across the entire vendor/product contract lifecycle with automated corrective action plans, remediation tracking, built-in evidence capture, and Board-ready risk summary reporting.
- In addition, HDOs leverage these solutions to manage enterprise risk, automating self-assessment of their own organizational coverage of recognized security practices like NIST CSF or HICP, and benchmarking cybersecurity program maturity and performance against peer organizations.

Healthcare Purpose-Built Risk Exchanges continued

Key Considerations (continued)

- These solutions offer flexible, scalable delivery models to HDO customers, from platform deployment to a full managed service to a hybrid platform/services model.

Best Practices for Evaluation

- Buyers should focus on the breadth and depth of healthcare-specific risk management use cases, including the volume and diversity of third parties on the exchange – this includes vendors, products, medical devices, IRB/research, biomedical, non-technical suppliers, as well as enterprise risk workflows for NIST CSF and HICP.
- Ecosystem integration and automation are critical components of evaluation across all solutions, including risk exchanges. Consider those solutions that enable the integration of third-party risk assessments into broader enterprise workflow & ticketing systems that drive faster innovation adoption without compromising safety or security.
- Buyers should compare other solutions to purpose-built risk exchanges across key metrics like time-to-value (in days), risk assessment time-to-complete (in days), return on investment, number of FTEs saved or redeployed through automation, and pricing/economic model; for instance, does the solution incentivize 100% risk coverage across the entire contract lifecycle – from procurement to renewal to retirement?

Final Thoughts

An American Hospital Association (AHA) Cybersecurity Preferred Solution Provider, Censinet is the first and only purpose-built risk exchange for healthcare that delivers fully-automated third party and enterprise risk management capabilities to HDOs to help them successfully manage, mitigate, and respond to today's cyber threats. If you would like to learn more, contact us at info@censinet.com or visit 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.