WHITE PAPER

VIGILOR
FROM TRIMEDX

Building the right cybersecurity strategy for your health system and technology assets

How health systems can internalize safety, success, and peace of mind

The expansion of network-connected technology in clinical environments has dramatically increased health systems' cybersecurity risk, as well as the potential threats to patient safety and continuity of care. Yet many organizations struggle to keep pace with their evolving needs. Many healthcare cybersecurity programs do not scale or adapt to the needs of medical device inventories and risk factors. Relying solely on external guidance like federal regulation will not be enough to deliver responsive, measurable results from cybersecurity projects. Adopting governance that is tailored to the unique needs of a healthcare organization may sound like an intuitive approach, but health systems face significant challenges to achieving this goal. In this white paper, we will examine what information health systems need to begin this process, where they can turn to source best practices for developing processes, and how they can apply both elements to establish a system of continuous improvement.

Reactive cybersecurity is not enough

It has become impossible to ignore the barrage of cyberattacks plaguing the healthcare industry. Hardly a week goes by without a major network breach making headlines, and too often the affected organizations are health systems. The warning signs are clear. Cybersecurity risks are now endemic to health care, and managing risk is only becoming more complex.

News of a cyberattack brings intimidating questions to mind. Were patients harmed? How will they recover? And what do we do if this happens to us? While these are understandable reactions, the list of questions that health systems need to ask—and answer—begins long before a breach occurs.

The average healthcare cyberattack cost nearly $10 million in 2023, twice as much as the average across all industries.[1]

Proactive cybersecurity questions

- What are our most pressing data security risks?
- How accurate is our inventory of technology assets?
- Have we identified all critical vulnerabilities? Are there remediations or mitigations available?
- What tools do we have to operationalize data and improve our risk posture?

Prioritizing preventative measures and acquiring data is key to shifting from a reactive to proactive cybersecurity strategy. Effectively engaging with these questions uncovers a flood of information. Many factors within a health system's own operations and from the broader healthcare technology industry create an organization's unique risk profile and security needs.

An increasingly dynamic risk landscape

One cyberattack method—ransomware—has dominated headlines and many industry conversations in the early 2020s, and that shows no sign of stopping. Ransomware exemplifies the terrifying increase in efficiency of cyberattacks. Instead of needing to access any specific type of digitally stored information to steal, ransomware seeks to lock authorized users' access to technology resources. As ransomware attackers can control data without removing it from health system's network, it is a troubling reminder of how abstract the reality of data ownership and possession can feel in the digital age.

Just as insidious are the methods that many cyberattacks, including ransomware, use to breach organizations. Social engineering is an approach that has made gaining access easier for many attackers. Instead of a stereotypical scene of hackers furiously typing code to break through firewalls, they now use deception to get permission to access networks. Spoofed email addresses, fake attachment links, and urgent language push employees to act without looking too closely. By the time they've realized that the communication is not legitimate, malware has already been introduced.

New technologies like generative artificial intelligence (AI) are making social engineering easier and more effective for attackers. AI can create a stronger incentive for an individual to engage with an attacker's communications by using professional and personal data to tailor deceptive content.[2] With knowledge of a target's schedule, behaviors, and preferences, AI-powered social engineering has the potential to identify organizational weak points more efficiently. In addition, generative AI reduced the manual effort in creating social engineering communications, meaning attackers can execute highly targeted efforts at a larger scale. Social engineering tactics turn every authorized user into a potential unwilling entry point for a breach.

At the same time, healthcare organizations also depend heavily on physical technology, otherwise known as the internet of medical things (IoMT). Medical technology requires many touchpoints to deliver benefits for patients and healthcare workers. This means a large inventory of medical equipment and IT devices tied together by a digital network. As technology has advanced, the technological footprint within hospitals has continued to grow. This complicates data security on two important fronts:

1. The number of devices that could threaten patient safety if compromised has grown precipitously.
2. It is far more challenging for health systems to track the location, status, and use of all their technology resources.

These conditions factor into the risks regarding high-profile cyberattack methods such as ransomware and social engineering. Yet there is also a significant physical risk frontier in clinical spaces of which health systems relying heavily on technology must remain vigilant. Removal of IoMT assets from secured, monitored environments exposes any stored data to unauthorized access, whether it is the result of any intentional act or human error. Just as opportunities for attackers have increased, so too are the opportunities for lack of oversight and human error to expose organizations to data breaches.

Efforts are constantly underway to combat the unique cybersecurity challenges in the healthcare industry.

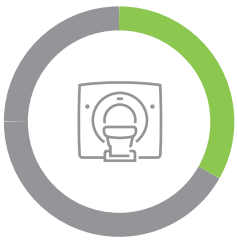
As medical device vulnerabilities are uncovered, manufacturers may or may not release patches to help close the gaps in security. New regulations may improve the availability of validated patches as well as security standards by which new technology and devices are judged. Yet as beneficial as these advancements are, they also represent a massive amount and rapid frequency of potentially actionable new information for health systems to digest.

So even if a healthcare organization takes the first step and asks challenging questions about their own cybersecurity strategy, how can they use the overwhelming amount of knowledge that this exploration brings?

In the absence of a robust cybersecurity framework tailored to the unique requirements of health care, organizations face several critical pitfalls. A reactive strategy that only address risk factors in the event of breach attempts can lead to significant challenges:

1. **Misplaced or unmonitored inventory:** Without a comprehensive inventory of networked assets, health systems can easily overlook critical systems, devices, or sensitive data. 74% of healthcare organizations now have more than half of their medical device inventory connected to networks.[3] Poor tracking of inventory can hinder timely threat detection and response.
2. **Longer remediation turnaround and backlog:** Reactive strategies often result in delayed incident detection, response, and remediation. Longer turnaround times can exacerbate vulnerabilities, allowing threats to persist and propagate within the network.
3. **Uncertain or hard-to-verify success metrics:** Reactive efforts lack clear success metrics. It becomes challenging to measure the effectiveness of security measures when actions are taken only in response to incidents. Quantifying improvements becomes elusive.
4. **Lack of effective vulnerability remediation before breaches occur:** Reactive approaches prioritize incident handling over proactive vulnerability management. As a result, vulnerabilities may remain unpatched, increasing the likelihood of successful cyberattacks.

74%
of health systems have **more than half** of their medical devices network-connected



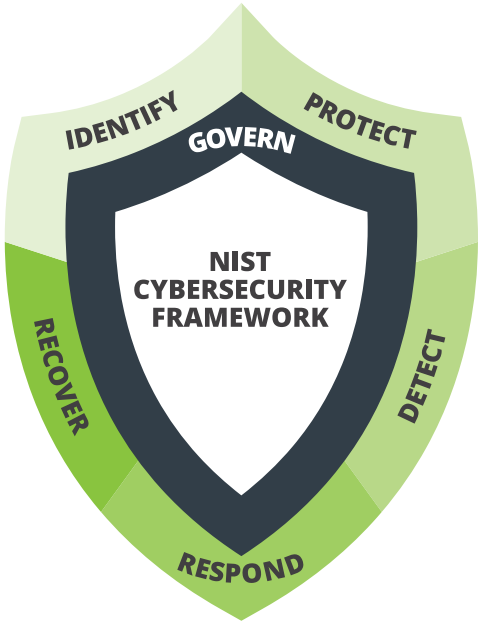
34%
of health systems have **7 out of 10 or more** of their medical devices network-connected

TRIMEDX internal data

Adding structure to healthcare cybersecurity battle plans

Taking a vast ecosystem of risk data and turning it into a productive strategy depends just as much on how it is done as what information is used. Consistent processes are the lynchpin to protecting operations, even before a breach occurs. Where should health systems turn for the starting point of building their cybersecurity framework?

In 2013, Executive Order 13636 leveraged the expertise of the National Institute of Standards and Technology (NIST) in establishing best practices for business operations to address the growing cybersecurity threats in nearly all industries.[4] The NIST Cybersecurity Framework (CSF) is a critical tool for organizations, including health systems, to manage and mitigate cybersecurity risks effectively. The CSF provides a flexible, repeatable, performance-based, and cost-effective approach to managing cyber risk. It is built on existing standards, guidelines, and practices, ensuring a wide range of applicability.



The core components of the Framework include:

1. **Identify:** Develop an organizational understanding to manage cybersecurity risk effectively.
2. **Protect:** Implement safeguards to ensure the delivery of critical healthcare services.
3. **Detect:** Establish activities to identify cybersecurity events promptly.
4. **Respond:** Develop procedures to act when a cybersecurity event is detected.
5. **Recover:** Create plans for resilience and restoration of capabilities or services impaired by a cybersecurity event.

Enhancing consistency with governance in NIST 2.0

NIST CSF Version 2.0 was published in 2024 and introduced a critical new component for the framework: Governance.[5] At first glance, this element might seem redundant, given NIST's strong focus on standardization of business practices. Yet the concept of governance is most crucial to how organizations that use the framework internalize not just the knowledge of best practices, but also the mindset of using consistent processes to apply guidance. This addition addresses the growing need for organizations to have a structured approach to rigorously collecting data from cybersecurity efforts and identifying the best approaches for remediating risk through repeatable actions. The principle of governance emphasizes the importance of leadership and management in establishing, supporting, and enforcing cybersecurity policies and processes.

Applying governance by uniting people and technology

The successful execution of a cybersecurity governance framework depends on health systems empowering their resources to scale and adapt with dynamic challenges. This synergy is particularly crucial in overcoming the challenges of inventory accuracy, a foundational element of a robust cybersecurity program.

A 2022 report revealed that 53% of healthcare IoMT devices, including medical equipment, have known critical vulnerabilities.[6] The challenge lies not just in identifying these vulnerabilities but also in accurately matching them to the relevant devices. This is where the combination of skilled cybersecurity professionals and advanced technology can make a significant difference, reducing false positives and enhancing actionable intelligence.

The integration of technology can streamline this process, making it less theoretical and more practical. It can help health systems establish and adhere to set processes, thereby improving cybersecurity maturity.

The vastness of inventories and the expansive geographic footprint of modern health systems require the use of technology. Manual accounting becomes an overwhelming task for teams already burdened with multiple responsibilities. Here, technology steps in as a valuable ally, simplifying tasks and enhancing efficiency.

The need for cybersecurity education is ongoing, keeping pace with the evolving landscape of hacking tools and methods. IT teams can actively engage with other members of the organization, fostering a culture of cybersecurity awareness. External third-party organizations well-versed in cybersecurity can also be valuable resources, especially for instructing clinical engineering teams on medical device cybersecurity.

In conclusion, the key to executing a successful cybersecurity governance framework in health systems lies in the unity of people, processes, and technology. Together, they can build a secure, resilient health system capable of withstanding the evolving challenges of the digital age.

Accepting cybersecurity risk as a multifaceted metric

To adopt stronger medical device cybersecurity policies, health systems need to gain full visibility of their inventories. Medical devices are complex, and the risks associated with them are equally intricate. Health systems should consider a wide variety of factors in evaluating the risk level of an individual device:

- Is a device capable of being connected to a network, and is it currently connected?
- How would an unexpected device failure endanger a patient?
- How will a device failure impact the ability to deliver care?
- Is the device displaying any anomalous network behavior?
- Can the device store ePHI?
- Does the device have known software vulnerabilities?
- Is patching support available from the device manufacturer?

Accepting this complexity empowers health systems to take confident action in understanding their unique risk posture. Establishing strong governance for a medical device cybersecurity program does not replace regulatory compliance. Rather, it equips health systems, their staff, and leadership with the tools to protect patients and their organization's reputation proactively.

1. **Mission**
   A clear mission statement ensures that incident response efforts align with the organization's overall goals. By adopting a governance framework, health systems can define their mission, emphasizing patient data protection and system resilience.
2. **Strategies and goals**
   Codifying strategy can improve alignment between personnel working towards organizational goals as well as understanding of top priorities. Health systems can tailor these to their specific context, such as improving incident detection, minimizing impact, and enhancing patient privacy.
3. **Senior management approval**
   Formal approval processes and consistent guidance from health system leaders ensure commitment, resource allocation, and alignment with organizational priorities.
4. **Organizational approach**
   A governance framework guides health systems in structuring teams and resources to best support their incident response approach. Roles, responsibilities, and cross-departmental coordination become clearer, leading to more effective incident handling.
5. **Incident response team communication**
   Clear communication protocols are essential. Health systems can expedite the work of incident response teams by establishing effective communication and fostering collaboration during incidents.
6. **Measuring capability and effectiveness**
   Health systems can measure their incident response capabilities using metrics and KPIs, identifying areas for improvement more confidently.
7. **Planning for growth**
   Scalability is crucial. Health systems can plan for increased incident volumes, expand their response teams, and allocate resources effectively.
8. **Integration with overall organization**
   The framework ensures incident response is not isolated. By integrating it into the organization's structure, health systems enhance overall security posture.

Despite the numerous risk factors that health systems must consider, repeated and standardized assessments can enhance overall risk comprehension. By establishing clear risk criteria, health systems can develop methods to quantify and prioritize risk for individual devices. This standardization enables health systems to better align the capabilities of their critical cybersecurity resources—people, processes, and technology—towards common goals. Well-trained associates following consistent steps and equipped with tools that simplify work have the best chance to respond to threats effectively as well as prevent them by managing risk.

Deploying these resources to perform regular evaluations creates opportunities for closed-loop improvements as remediations are implemented and devices evolve over time. This approach enables health systems to monitor progress, promptly identify significant risks, and continuously enhance their risk posture. Ultimately, a quantitative, closed-loop approach helps health systems proactively manage medical device risk and stay ahead of regulatory requirements.

While regulatory and legal compliance are crucial for mitigating cybersecurity risks in health systems, modern cybersecurity risks demand more. Health systems should adopt a comprehensive approach by implementing robust internal governance. This integration allows them to align compliance efforts with their unique risk profile and cybersecurity needs. With a dedicated focus on medical device cybersecurity, health systems can better safeguard patients, operations, and their reputation.

SOURCES

1. *IBM. Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach*
2. *Heiding, F., Schneier, B., Vishwanath, A. AI Will Increase the Quantity — and Quality — of Phishing Scams. Harvard Business Review. https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams*
3. *TRIMEDX internal data*
4. *National Institute of Standards and Technology. History and Creation of the CSF 1.1. https://www.nist.gov/cyberframework/history-and-creation-framework*
5. *National Institute of Standards and Technology. NIST Releases Version 2.0 of Landmark Cybersecurity Framework. https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework*
6. *Health IT Security. (2022). 53% of Connected Medical Devices Contain Critical Vulnerabilities. https://healthitsecurity.com/news/53-of-connected-medical-devices-contain-critical-vulnerabilities*