POINT OF VIEW

Healthcare Provider Industry Merger and Acquisition Activity Means Increased Cybersecurity Risk

Healthcare providers are increasing their merger and acquisition activity. They are motivated by competitive advantage, reductions in reimbursement rates, and service offerings enhanced in new markets. While great for consumer access, this activity can also increase security risks. Fortunately, there are strategies and security solutions to help minimize and mitigate the threats that may come with provider mergers and acquisitions to keep sensitive patient information, Internet-of-Medical-Things (IoMT) technology, and patient data secure.

IoMT and Cybersecurity Threats to Healthcare Providers

The information technology (IT) complexity that comes with a merger or acquisition within the provider space poses a major cybersecurity risk. That risk carries over to the modalities and devices that provide services that are considered IoMT as the two different networks within these systems converge. In fact, healthcare providers are under increased attacks as a breach risk than those in any other industry, with the proliferation of connected medical devices, consumption of eletronic medical records (EMR) and hybrid cloud technologies, and the acquired entity will know long in advance they are being acquired and will build up technical debt due to lack of investment.

Cybersecurity Imperatives for the Healthcare Provider Space

When it comes to cybersecurity, there are a number of imperatives facing the provider space. Of course, it all starts with protecting patient data and operations. Security breaches can decimate the staff, company reputation, and ability to provide operations. Breaches can result in fines, inability to provide services, and additional workloads on an already understaffed security operations team. All of this adds up to billions of dollars in liabilities. So, what can be done to minimize and mitigate the cybersecurity risks associated with these mergers and acquisitions?

As healthcare providers grow larger and more complex, they must unify their cybersecurity strategy and take into consideration the needs of both IT and IoMT. Many providers have aging and separate IT/IoMT management that present operational and security challenges, posing a risk to everything from hospital operations to billing and documentation. In addition, failure to adequately protect against cyber threats and demonstrate compliance with multiple regulations and standards can not only result in lost patient data but also in hefty fines. End-to-end security integration across the entire

cyber-physical landscape, especially for IT and IoMT silos, allows for greater transparency and visibility into impending threats as well as seamless upgrades as regulations evolve.

Last of the imperatives is the debate over incremental change vs. a rip-and-replace strategy when acquiring new, or maintaining, legacy technology. The reality is that the provider space has no appetite for total replacement, because no organization can afford a disruption in operations, supply chains, and patient care. This results in a mix of old and new technologies and all of the vulnerabilities that come with the inconsistencies inherent in that type of structure. Healthcare providers must protect the legacy technology as they incrementally upgrade to new, innovative solutions. Every part of the process must not be disrupted since patient care, patient satisfaction, and employee satisfaction is their business and what drives it. The Fortinet Security Fabric provides a single-vendor, end-to-end, integrated cybersecurity architecture across IT and IoMT, from prevention to protection to detection to response.

Cybersecurity Best Practices for Healthcare Providers Involved in a Merger and/or Acquisition

A major issue with the increase in the number of mergers and acquisitions within the provider space is that acquisition targets rarely, if ever, possess adequate security infrastructure. The phenomenon is well known but remains a persistent challenge. Such mergers and acquisitions need to consider cybersecurity best practices as part of connecting to an already complex web of affiliated and unaffiliated hospitals, clinics, and supporting facilities.

These provider hospitals, clinics, and labs routinely access and transfer patient data, electronic protected health information (ePHI), and other sensitive Health Insurance Portability and Accountability Act (HIPAA) data. Owing to their disconnected systems, healthcare provider enterprises struggle with challenges of visibility, data control, access auditing, and compliance reporting throughout their networks. In addition, when two different systems are consolidated, the results are often inconsistent and potentially incomplete, while the perimeter and threat surface continually expands. But with these challenges come opportunities. Healthcare providers must learn to adopt a practicable approach to augmenting security, bringing consistent and complete risk mitigation, total assurance, and the ability to thrive as they grow, merge, divest, and acquire new facilities.

Conclusion

Mergers and acquisitions are a regular occurrence in the healthcare provider space, and this poses a unique challenge from a cybersecurity perspective. If a provider's valuable data is compromised or improperly protected, that could threaten a merger or acquisition before it becomes final. When companies are integrated, their cybersecurity strategies and solutions are rarely aligned, and the transition brings swift changes to security and increases the risk of exposure to threats.

Even when healthcare providers are not involved in a merger or acquisition, they face cybersecurity challenges ranging from network complexity to antiquated IoMT systems to compliance. But there are cybersecurity systems designed to help keep complex providers cyber secure. An important step in solving complex security issues is to take a holistic architectural approach to network security. This will provide the visibility, automation, and fast response to threats required to thwart attacks and easily demonstrate compliance.

Read more about how the Fortinet Security Fabric provides a single-vendor, end-to-end, integrated cybersecurity architecture across IT and operational technology (OT), from protection to detection to response.

Reach out to healthcare@fortinet.com for more information.

July 23, 2021 3:21 AM
1172202-A-0-EN