LONG 80™
A GAVS & PREMIER, INC. JV

White Paper

Security Challenges and Emerging Trends in Healthcare

Kavitha Srinivasulu

Head Cyber Security & Data Privacy - Healthcare

Digitalization of Healthcare

With the industry moving towards healthcare transformation and 'digital health', there has been a lot of innovation and shedding of legacy systems & processes. EHRs (Electronic Health Records) and Telehealth are enabling greater healthcare interoperability and mobility. But, with the healthcare industry still learning the ropes of newer technology, it has not yet fortified data and system security in equal measure. This has provided an easy path for cybercriminals to exploit these vulnerabilities and target the Healthcare Industry.

Security Challenges in Healthcare

The rise of ransomware threats

The global ransomware damage runs to billions of dollars each year and has been increasing steadily. About 26% of respondents to the 2021 Consumer Healthcare Cyber Security Threat Index expressed concern over ransomware attacks shutting down access to healthcare. Ransomware attacks such as phishing emails, malware advertisements can lead to debilitating financial & reputational implications and disrupt the treatment patients are entitled to. Another reason for the steady rise in ransomware attacks is the rise in the price paid for sensitive patient information and medical records in the dark web markets.

AI-based cyberattacks

One of the reasons why healthcare as an industry, is a prime target for a cyberattack is its reactive approach to data security and privacy. Cybercriminals are becoming increasingly savvy in the use of technology to design sophisticated attacks. They leverage AI and ML to create Advanced Persistent Threats (APTs). The use of such technologies doesn't require rocket science skills, with the availability of varied off-the-shelf AI/ML models. This helps them launch cyberattacks with such variety and rapidity that wouldn't have been possible through manual means. These forms of cyberattacks remain unnoticed as they are introduced into the system masked as legitimate updates or security patches. If the healthcare provider's IT firewall is weak, if the team is understaffed, or proactive security measures have not been implemented, these AI threats can set up camp, quietly build their network and expand their footprint until it is too late to notice and take recovery measures.

The emergence of IoMT and health devices

The usage of connected devices and monitors helps healthcare professionals provide holistic care by leveraging comprehensive patient data. The use of such devices with data transmission over networks, and with the increasing implementation of BYOD (Bring Your Own Device) policies without the accompanying safety measures, puts personal and sensitive data at risk, to say the least. If such devices are not properly managed and monitored, it could lead to a greater problem of shadow IT wherein the IT team isn't even aware of the existence of such devices in their network and hence they would not fall under IT's purview. Mismanaged device firmware, system software, application software, configurations, and policies, lack of a powerful firewall etc., further facilitate hackers to find loopholes and intercept records with ease, violating federal patient privacy laws.

Patient-centric business model

With patients taking a more proactive role in their own health & wellbeing with the use of healthcare devices, apps, and with clinicians having access to integrated, 360° information about each patient, the quality of care has enhanced drastically. This has been made possible through use of integrated systems and data modernization that enables sharing and interoperability of the data. But the downside to this is that there is a lot of data movement over networks, across systems and applications, resulting in more chances of data exposure. This patient-centric approach will be sustainable over the long term only if healthcare players invest in the right platforms that facilitate seamless and secure communication of data.

Government Intervention to Combat Rising Security Threats

Due to the rise in the number of security threats against the healthcare industry, the U.S. Department of Health and Human Services (HHS) established several laws that focus on data breaches, patient's right to privacy, and misuse of privileged information. Some of them are —

- Governed by the HHS Office for Civil Rights, the **Health Insurance Portability and Accountability Act (HIPAA) of 1996** protects sensitive patient health information from being disclosed without the patient's consent or knowledge.
- The **Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009** focuses on privacy and security protection available under HIPAA compliance.
- **HITRUST** is a framework that includes 149 control specifications, incorporating requirements from NIST, ISO, and HIPAA supporting an organization's information risk management and compliance program.

Emerging Trends to Mitigate Security Issues in Modern Healthcare

Inventory visibility and management

To implement a robust cyber security system, automation is critical. Healthcare organizations must develop a detailed device inventory in the order of vulnerability to formulate a strategy to mitigate security issues. Inventory management focuses on having a clear and deep clinical understanding of each device, patient safety classification, and the healthcare workflow from a healthcare perspective.

Medical device visibility

Lack of visibility to the entire range of medical devices can create havoc and undermine the security measures of the healthcare organization. Hospitals must implement cyber security solutions that offer end-to-end visibility for potential cyberattacks or intrusions. Performing a complete audit of the list of medical devices will help select and implement network security control and review.

Use of AI/Automation

With increasing digitalization, healthcare mobility, BYOD options, IoMT, etc. healthcare infrastructure has become very complex. The peripheries of a healthcare organization have now moved well beyond physical boundaries. Due to this, effective management and securing of health infrastructure assets necessitate the power of Artificial Intelligence, Machine Learning, and Automation to supplement human capabilities. AI/ML techniques can be effectively used to 'discover' the IT landscape, to analyze huge volumes of data and eradicate noise from the data and detect anomalies in behavior patterns. Most importantly AI/ML can be used to drive proactive detection, prevention, automatic remediation, and rapid management of security incidents.

Enablement of secure mobility

While telehealth and clinician mobility are taking healthcare to new heightened realms, the security challenges these technologies pose need to be given special attention. The use of the right technologies and products which come with in-built security features and which can integrate seamlessly with additional 3rd party security layers, can make all the difference.

Vendor management

Having a large number of security products results in security silos, complexity, increased integration costs, and complex staffing requirements. Consolidating the number of touchpoints and vendors will help improve security risk posture through integrated systems & platforms and better visibility into the threat landscape.

Stringent policies and guidelines for data and infrastructure governance

Based on Gartner's 'Top Security and Risk Management Trends 2021', Long 80 recommends the following methods to mitigate and manage security issues:

- CISOs must start focusing on breach and attack simulation (BAS) tools that will help identify and mitigate gaps in the security landscape.
- As per the Gartner 2021 Board of Directors Survey, cyber security is considered the second-highest source of risk. To that end, healthcare enterprises must focus on creating a dedicated team committed to addressing cyber security issues at the board level.
- Eliminating silos at the security level will improve the overall firewall setup of the infrastructure. Implementing a cyber security mesh with centralized policy management will ensure that the security protocols reach even distributed assets.
- Revisiting policies governing data protection, data disaster backup, and recovery is crucial to remote work mode of operations.

Future of Security in the Healthcare Industry

The dependency on technology in healthcare is on the rise. As more data gets collected, shared, and analyzed, cyber security and data privacy need to be prioritized. Healthcare players must understand that security and privacy are no longer just for the sake of regulatory compliance but are quintessential for the safe day-to-day functioning of the organization. As data protection and patient safety became imminent, the healthcare industry must focus on

- Upgrading or replacing legacy systems
- Complying to legal and regulatory requirements
- Regular cyber security awareness and training programs
- End-to-end security risk assessment & analyses
- Increasing budget allocation for cyber security and data protection

Long 80's expertise in AI, ML, and Big Data Analytics empowers healthcare organizations with proactive and secure digital transformation. Long 80 offers best-in-class cyber security and data privacy solutions delivering exceptional client experiences that directly result in competitive advantage, cost-savings, growth, and improved operational efficiencies to healthcare service providers.

To learn more about our offerings, please visit https://long-80.com/.

LONG 80™
A GAVS & PREMIER, INC. JV

Long 80, LLC. is a collaboration between GAVS Technologies and Premier, Inc. on a strategic joint venture.

Premier, Inc. is a leading healthcare improvement company headquartered in Charlotte, NC, and GAVS Technologies N.A. (GAVS) is focused on Artificial Intelligence for IT Operations (AIOps)-led managed services and digital transformation. Long 80 will bring innovative, AI-driven information technology (IT) operations and security operations to healthcare organizations in the US.

To find out how Long 80 can help your organization, please visit www.long-80.com or write to inquiry@long-80.com.