Improving digital trust in the healthcare industry

With increasing willingness to use wearables and share personal information over the web, patients want healthcare to be delivered as a service. Healthcare providers are catering to these expectations by building their digital ecosystem, with around 60% of them having made this a top priority. Availability of Protected Health Information (PHI) and Personally Identifiable Information (PII) over the Cloud has proliferated leading to innumerable cybersecurity challenges.

Compliance requirements like Health Information Portability & Accountability Act (HIPAA), General Data Protection Regulation (GDPR) etc. have increased CISO/Privacy Officers' focus towards protecting PHI & PII data. Proliferation of Internet-of-Things (IoT) and mobile devices in healthcare has expanded the attack surface several fold. The rise of highly innovative and sophisticated fraudsters coupled with non-availability of skilled talent to counter new types of attacks has amplified the challenges associated with ensuring a secure digital ecosystem.

Two examples to illustrate the extreme damage that can be caused by hackers are:

- Wannacry ransomware attacks on healthcare institutions resulted in $ 100s of million losses
- Multiple instances of insulin pump cyber bug deliberately overdosing diabetic patients leading to their deaths

Some key practices that healthcare companies should adopt to enhance digital trust are:

- Cloud security compliance assurance program
- 3rd party risk assessment and compliance program
- Secure by design
- 24/7 managed detection & response services
- Regular cyber resilience assessment

60% of organizations believe that a bad cyber security event will lead to significant fines or sanctions due to non-compliance

Cloud security compliance assurance program

Healthcare companies have to ensure secure storage and usage of sensitive patient data. Added to this are complexities related to multiple cloud systems connecting with each other within the healthcare ecosystem and advanced threats targeting them. It is best to adopt a common control framework incorporating the various regulations and standards governing the healthcare industry. A risk based approach is needed to decide on appropriate controls as required by the business. Blanket enforcement of all controls will be cost prohibitive. The risk assessment model used needs to use adequate change controls, traceability and auditable configuration controls. After the initial assessment and remediation, healthcare organizations must adopt automation methods to make continuous compliance to industry regulations and standards a painless process. Doing this can help healthcare companies improve their cybersecurity preparedness in an ongoing manner.

3rd party risk assessment and compliance program

Changing patient expectations to deliver healthcare as a service has resulted in digital mobile engagement between the patient, hospital, doctor, insurance company and the pharmaceutical company. Such a distributed and seamlessly connected ecosystem has enhanced the chances of cyber breaches. Studies have repeatedly thrown up the fact that 41-63% of the breaches involved 3rd parties. Therefore healthcare companies need to adopt an integrated 3rd party risk assessment and compliance program.

A robust 3rd party risk assessment and compliance program should classify vendors according to their criticality based on business impact and use different risk assessment questions and controls depending on their criticality. Typical domains based on which the risk assessment is done are digital, cloud, financial, geo political, information security, human rights, privacy laws, health and safety and environment. A custom made risk scoring methodology is used based on the specific vertical the healthcare company belongs to and a weighted scoring method is used based on the responses across each of the domains. Threat feed information from external sources can be used to arrive at the overall risk score. Both domain based scores and the overall score should be factored while taking remediation decisions. Finally automation of this process will ensure repeatability and smooth functioning of the process on a continuous basis.

Secure by design

Medical device manufacturers and pharmaceutical companies operate in a highly regulated environment. The proliferation of IoT usage in this industry has underlined the need for ensuring continuous operational security. The usage of over the shelf software with a different

lifecycle compared to the underlying device and the ever changing threat landscape during the lifecycle of the equipment has made 'secure by design' an imperative process rather than a nice to have process.

Secure by design process involves the implementation of Secure Software Development Lifecycle (SSDLC) principles in the manufacture of medical devices and pharmaceutical manufacturing equipment. Food and Drug Administration (FDA) and European Union (EU) regulations and laws are applicable in this industry. During the software design stage STRIDE threat modeling framework is used to ensure a secure design. STRIDE checks for security threats around six categories of security threats – Spoofing of user identity, Tampering, Repudiation, Information disclosure (privacy disclosure or data leak), Denial of service and Escalation of privilege. Continuous vulnerability assessment and penetration testing using FDA & EU medical device and pharmaceutical industry regulatory controls and the popular OWASP top 10 and SANS top 25 vulnerabilities library ensures comprehensive security testing of the software under development. Immediate remediation of the identified vulnerabilities will ensure the software, when it is fully developed, is almost vulnerabilities free. This will make it almost impossible for hackers to gain access to the medical devices and pharmaceuticals manufacturing equipment to perpetrate their malicious acts.

24/7 managed detection & response services

With innovative hackers on the rise and potential financial losses due to cyberattacks touching 100s of millions of dollars, it is important for healthcare companies to put in place 24/7 threat intelligence and detections systems. Security Information and Event Management (SIEM) tools are typically used to keep track of network traffic and provide real time analysis of potential threats and trigger security alerts for taking appropriate action. These tools are programmed to look for use cases developed based on typical cyberattacks. Some typical examples of use cases are – repeated failure of login attempts, repeated scanning of firewall ports from a single IP, malware check and detection of insider threat.

Nowadays anomalous behavior based SIEM tools that look for potentially malicious behavior, identified using continuous threat feeds, are gaining ground. This is an improvement from the purely use cases based methodology as it can lag behind creative hackers who develop new techniques on a continuous basis. This uses threat hunting techniques in which humans based on information provided by continuous intelligence feeds actively chase down hackers by identifying malicious behavior early in the attack cycle. They then take evasive action to prevent such cyberattacks from progressing. threat hunting uses a cyber kill chain model which systematically tracks down potential attacks through its different stages.

Healthcare companies using managed detection and response services can ensure they are one step ahead of fraudsters and thereby keep their data, IT infrastructure and operations safe.

Regular cyber resilience assessment

Major cyber breaches can result in damage to reputation of the enterprise, disruption in business operations, financial losses and erosion of trust placed by customers. This necessitates adequate organizational preparedness to handle such breaches and recover from them quickly.

An ideal cyber resilience framework should use a six stage approach:

Prepare – Understand the organization and its cyber risk landscape

Protect – Develop appropriate strategies and controls to effectively manage them

Detect – Put in place processes to identify anomalies and breaches. Conduct regular control testing to identify control breaks

Respond – Once a breach is identified the organization should deploy an incident response process. For major incidents an appropriate crisis management process involving C level management should be deployed

Recover – Business continuity and disaster recovery processes should be invoked to move to business as usual once the situation has been stabilized

Improve – Once the organization recovers and moves to normal business operations it needs to do a root cause analysis to identify what went wrong and derive learnings from it.

The cybersecurity practices listed above are reasonably comprehensive and will help healthcare companies improve digital trust. Thereby the digital ecosystem can be leveraged to provide better and safe patient care.

About the author

Kannan
SBU Practice Director and Head -
Health and Communications,
Wipro Limited.

Kannan has 17 years of experience in the cybersecurity domain as a business leader and has rich experience in starting and building the cybersecurity business in several companies. He has experience in starting and building the cybersecurity business into a multi Practice business stream consisting of Identity & Access Management Services, Application Security & Infrastructure Security Testing Services, Governance, Risk & Compliance Services and Global Security Operations Services including Managed Detection & Response Services.

Kannan has a Bachelor of Engineering degree and a MBA in marketing.

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035,
India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 175,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**

IND/B&T/SEP2019-FEB2020