



Does the healthcare industry have healthy cybersecurity?

The healthcare industry is vast, with a range of various organizations performing the most critical, complex and data sensitive operations that all relate to our wellbeing. As such, this industry obtains highly unique, significant data. The value of the data within the healthcare industry, which is largely PHI (Personal Health Information), can sell for over 100x more than PII (Personally Identifiable Information) on the black market, making this sector an attractive target for bad actors. Today, the healthcare industry is benefitting from a close relationship with technology thanks to all the advantages it has provided hospitals, pharmacies, laboratories and more. However, this means greater risks of cyberattacks occurring. The healthcare industry suffered from 365 data breaches in 2018 (that's one a day!), with over 13 million records being exposed. The health sector is also susceptible to malware attacks, especially those of ransomware attacks, which make up 39% of malware-related attacks. Ransomware attacks will encrypt the target's data until a payment is made, whereby the decryption key still only might be provided.

Rogue devices are becoming an increasingly used attack tool due to their invisibility to security software since the attack occurs on the Physical Layer. Spoofed peripherals that are attached to an organization's network or endpoint can perform exfiltration and injection actions, thereby allowing for data to be withdrawn, or malware installed.

Risks

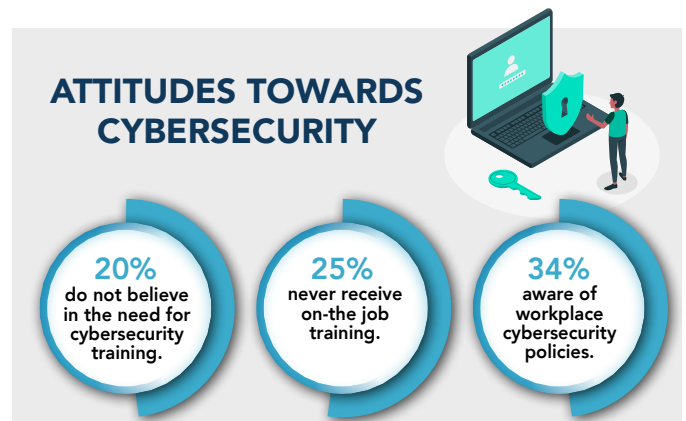
One might assume that an industry which relies so heavily on technology would also implement high levels of security. Wrong. The primary focus is on patient care, rather than cybersecurity. It is argued that the often-critical nature of the healthcare sector means users need immediate access to equipment and databases, thereby explaining why the internal perception is that greater security would be detrimental to operations. As such, these attitudes have led to the industry heavily lacking in sufficient cybersecurity measures thereby making an already difficult-to-detect attack even more challenging to mitigate. Insiders can also be the cause of a cyberattack; unwittingly or not. Malicious employees, or those who have been socially engineered, may bring a rogue device inside the premises

for it to ultimately be used by them, or other staff members. Furthermore, IoT and BYOD have provided bad actors with greater access points to an organization's network, making it easier to carry out a rogue device attack. The supply chain also presents a risk to any organization, especially the healthcare sector which relies heavily on third parties, of which most are exposed to sensitive data. Rogue devices may be sent into the organization via its supply chain, or the supply chain itself could be the target as it is sometimes easier to infiltrate.

Consequences

The consequences of a cyberattack are often financial-related; directly and indirectly. For the healthcare industry, the fines that accompany a data breach are often in the eight-figure range, in addition to reputation-building costs, of which hospitals spend around 64% more on annually than other breached sectors. However, in addition to this, the consequences within the healthcare industry can also be fatal in the long run.

A study found that when a hospital is hit with a cyberattack, the quality of that hospital diminishes, which, as a result, causes greater patient deaths. Focusing resources on cleaning up a data breach can lead to a lack of attention being given to the patient's wellbeing which can ultimately be lethal.






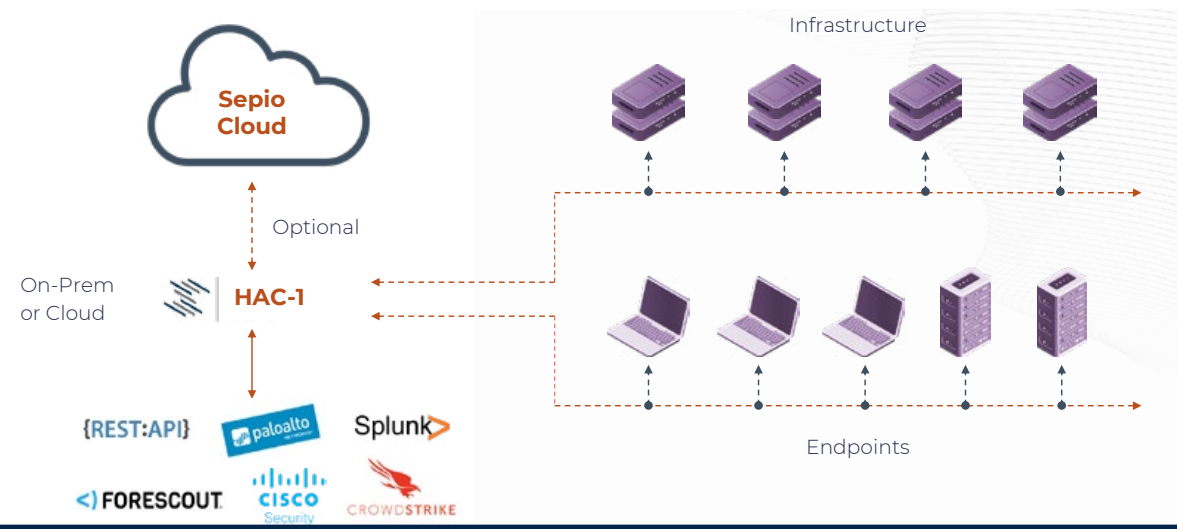
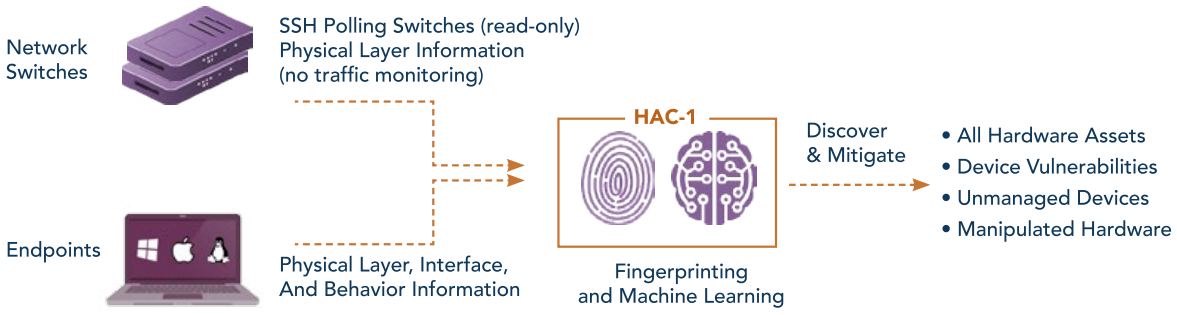


Rogue Devices

Rogue devices are peripherals which have been manipulated to act with malicious intent. They have the ability to carry out various types of malware attacks, including ransomware attacks, and data breaches. The aforementioned vulnerabilities of critical infrastructure can all be exploited by rogue devices, making them a useful attack tool for perpetrators, but a dangerous enemy for the victim. Most importantly, these devices not only look genuine to the human eye but also go undetected by security software solutions which simply identify them as legitimate human interface devices (HIDs), such as a mouse or a keyboard, and therefore will not raise any EPS/EDR alerts. Network implants and Spoofed devices attacks occur on the Physical Layer (Layer 1), which the existing security software, mainly NAC and IDS does not cover.

Main Benefits of HAC-1

- 
Complete Visibility of all Hardware Assets: With all devices and anomalies detected, enterprises benefit from a greater overall cybersecurity posture. Gaining full visibility of all hardware devices from endpoint peripherals to connected devices (IT/OT/IoT), Sepio uses unique physical layer hardware fingerprinting technology and data augmentation from endpoints and networks.
- 
Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.
- 
Rogue Device Mitigation (RDM): Threat mitigation upon discovery of rogue or threatening devices. Integrations with existing security platforms such as NACs and SOARs for mitigation and remediation enhancements.



www.srccybersolutions.com

+91 120 2320960

sales@srccybersolutions.com



ABOUT SEPIO

Founded in 2016 by cybersecurity industry experts, Sepio's Asset Risk Management (ARM) platform sees, assesses, and mitigates all known and shadow assets at any stage. The only trafficless solution, Sepio is infinitely scalable to protect the company's decentralized, uncontrolled ecosystem as fast and often as anyone, anywhere connects any assets. Sepio provides actionable visibility with the Asset Risk Factor (ARF) score based on a unique Asset DNA generated for each asset at its physical source, reflecting actual business, location, and rules. Sepio radically improves the efficacy of NACs, EDRs, XDRs & Zero Trust layer solutions that simply see only the assets they are there to protect. Visit: www.sepiocyber.com.

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Highly Automated, and User-Friendly Solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONScales for Comprehensive Email Security and Anti-Phishing Protection, SEPIO for Asset Risk Management (ARM) to assess and mitigate all known and shadow assets at any scale, THREATX for WAAP (WAF++) for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

