Pharmaceutical

A Sepio white paper

SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Pharma Industry Challenges Amid COVID-19 Pandemic

The pharmaceutical industry is one of the most vital industries in the world; discovering, developing, producing and marketing drugs and medication to help patients suffering from illnesses as minor as the common cold, to life threatening diseases such as cancer. Especially today, when COVID-19 is causing major global disruptions, the world is relying on pharmaceutical manufacturers to conduct research and development into a vaccine.

A study conducted by Deloitte found that the pharmaceutical industry is becoming the number one target for cybercriminals around the world. Because of the nature of the industry's work, the type of information and data obtained by pharmaceuticals is extremely valuable and, as such, highly appealing to bad actors. It is not only financially motivated criminals that target the industry; state-sponsored groups are the most common perpetrators who aim to steal data in order to gain a competitive advantage. In an industry where innovation takes years, and costs millions of dollars, stealing intellectual property fast tracks competitors without them having to do any of the groundwork. And the current COVID pandemic means that pharmaceutical companies conducting related research or support need to be extra vigilant.

Attacks

IP Theft

One of the main motivations behind a data breach is to gain financial benefits. With pharmaceutical manufacturers having access to an abundance of patient information, bad actors who steal this data can make a fortune on the black market. In early 2020, ExecuPharm suffered a data breach whereby social security numbers, taxpayer IDs, driver's license numbers, passport numbers, bank account details, credit card numbers, NI numbers and beneficiary information were stolen. Moreover, because of the connectedness between ExecuPharm and its parent company Parexel, data from the latter was also stolen. This is clearly a massive security breach and the perpetrators can benefit from a huge pay-out by selling such information on the dark web. Additionally, IP can be stolen and sold for a substantial amount, and IP theft is the main goal for bad actors targeting this sector.

However, the financial gains associated with IP theft are often secondary to the competitive advantage gains that come with such an attack. Often, state-sponsored attackers are trying to gain technological or commercial advantages for their country's economy.

In China, for example, there is an aging demographic and rising cancer rates which have spurred the Chinese Communist Party to develop its pharmaceutical industry; however, this is no easy task. Due to the crucial IP owned by pharmaceutical companies that relates to new drugs and medicines, having been developed over years and with heavy financial investments, it comes as no surprise that Chinese state-sponsored hackers are often found to be the perpetrators of IP theft and espionage in order to advance in this sector. In 2018, a Chinese biochemist pleaded guilty to stealing trade secrets from drug manufacturer GlaxoSmithKline, and in 2019 his brother was charged with corporate espionage in the pharmaceutical industry.

It is not just China that is often associated with pharmaceutical IP theft. Russian hacking group Dragonfly has, in recent years, become more focused on stealing IP belonging to pharmaceuticals.

Ransomware

When a ransomware attack occurs, systems and files are encrypted until a ransom amount is paid. This is extremely damaging in the time-sensitive pharmaceutical industry. The 2017 NotPetya attack on Merck caused worldwide operational disruptions which resulted in the company halting the production of new drugs. Similarly, the WannaCry attack in the same year caused healthcare systems worldwide to shut down, including those of pharmaceutical companies. Production disruption is particularly damaging due to the critical nature of the industry's operations. Furthermore, it is not guaranteed that the encrypted files will be retrieved, meaning that the victim organization is at risk of losing all of the encrypted data. For the pharmaceutical industry this can be a significant setback in drug development and clinical trials, should this data not be recovered.

Malware

The injection of malware can cause of number of perilous attacks, including the aforementioned data breach and ransomware attacks. Last year, Swiss drug manufacturer Roche was attacked with malware, as was Bayer in a separate incident.

Both attacks were attributed to Chinese state-sponsored hacking group Blackfly, but thankfully no data was stolen. Nonetheless, these attacks are just two recent examples of how state-sponsored groups are turning their attention to the pharmaceutical industry, and an even greater example of how pharmaceutical organizations are not protected against such an attack.

Risks

Technological developments

The reliance on robotics, AI and IoT throughout the industry means that the pharmaceutical sector is more at risk than ever. The industry sees technological advancements; bad actors see a greater number of entry points.

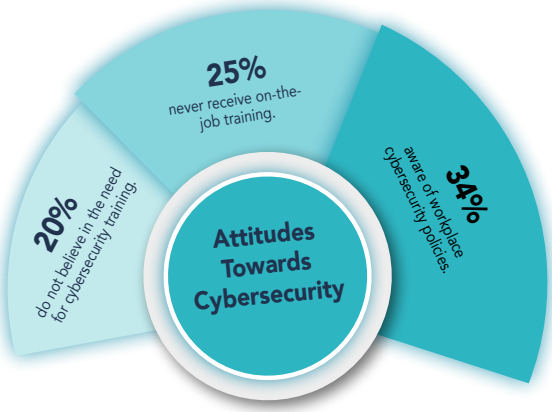
With the connectedness of IT and OT networks, an attack on one can easily spread throughout, making the attacker's job that much easier since they only need to gain access to one device.

Moreover, digitization means that more valuable data is being stored online, thereby making the appeal of an attack even greater since the payoffs are higher.

Supply chain

With more systems now connected to the internet, they can be accessed by third party vendors. Because of this interconnectedness, just one broken link will compromise the entire chain. Again, by simply gaining access to one component, attackers can move laterally throughout the network and will often target suppliers in order to do so since they are viewed as an easier target. In 2014, Dragonfly was found to be targeting small companies that supplied the pharmaceutical industry as an easier way to infiltrate the sector.

However, a third party might not be acting unwittingly. The ability for suppliers to access the primary organization's network means that malicious employees are able to conduct attacks due to their insider privileges. And, with less control over the organization's data, there is less visibility as to who has access to what and how that information is being used, thus facilitating a third-party insider attack.



Insiders

Following on from above, insiders within the pharmaceutical manufacturer pose the same risks. Vindictive employees are a major risk, yet unaware and negligent staff are also a huge threat.

A lack of awareness regarding cybersecurity is a serious vulnerability since employees will be oblivious to warning signs of an attack, notably social engineering tactics. Furthermore, untrained staff might act in ways which only increase the organization's susceptibility to an attack purely based on the fact that they do not obtain the necessary knowledge on cybersecurity. Even if there is a cybersecurity strategy in place, it is only effective if employees know how to implement it correctly.

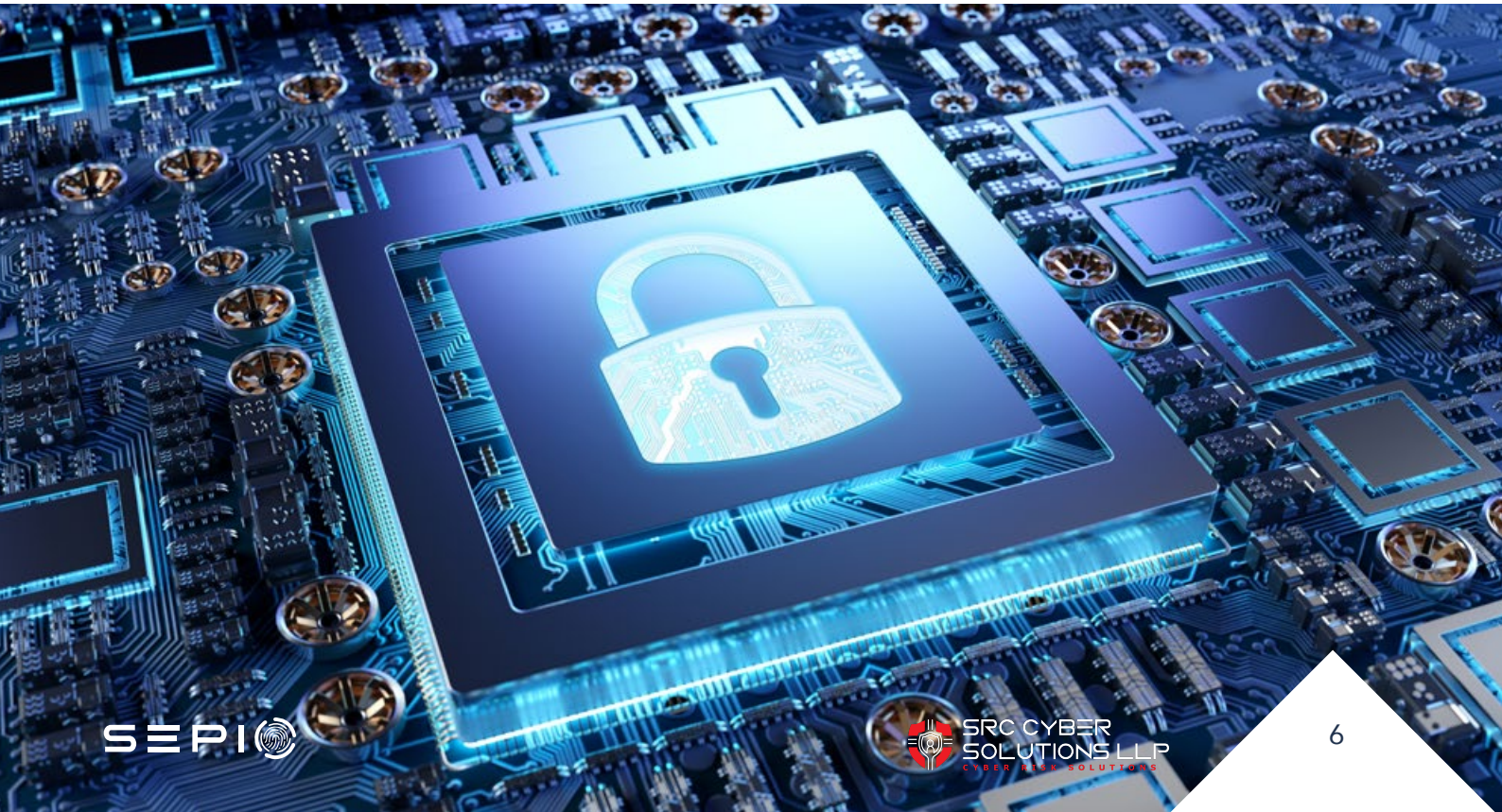
Rogue Devices

Bad actors are making use of Rogue Devices to carry out attacks, including those mentioned above. Rogue Devices are those which have been manipulated to act with malicious intent.

By using the hardware attack interface, bad actors have increased chances of success since they go undetected. Hardware Implants sit on the Physical Layer, thus going unnoticed by existing security software solutions; and spoofed peripherals will be recognized as genuine devices, while executing the attack through a USB HID interface, or a spoofing MiTM network device thereby raising no alarms to the security department.

The covert nature of such devices, and the range of their capabilities, makes them a perilous threat to the pharmaceutical industry, which is already a top target.

With attackers always seeking to find new attack tools, the pharmaceutical industry is most definitely at risk of being a victim. And, without any protection against such devices, the threat is only magnified.



Consequences

Financial Costs

The financial costs associated with an attack are both direct and indirect, of which the latter can last for years following the incident. Primarily, the cost of a ransomware attack includes the ransom payment, should the victim choose to pay it. And, in the time-critical pharmaceutical industry, there is often no time to consider alternative options. Importantly, there are often legal costs the come following an attack both in the form of fines and lawsuits. The operational disruption associated with an attack will result in a loss of revenue that is made up of downtime and supply chain shortages. Moreover, clean-up costs add to the financial burden of an attack, including that of repeating research and clinical trials, and advertisement costs aimed at repairing reputational damage.

Reputational damage

The aforementioned reputational damage can be severe in the pharmaceutical industry, due to the critical nature of their operations. The success of an attack demonstrates vulnerabilities in the organization's security, and this will not be taken lightly by stakeholders. Importantly, this will erode consumer trust and this can sometimes be impossible to recover from.

Operational disruption

With the industry relying so heavily on IT and OT, a cyberattack can stop production, research, clinical trials and more. As mentioned, the industry is extremely time sensitive, hence any disruptions that cause productivity and operations to be halted will have a major effect on ability to supply products. Furthermore, should a supplier suffer from operational disruption, this will have a spill over effect on the entire chain.

Patient safety

Importantly, patient safety can be compromised as the result of an attack. Stolen credentials can have a major impact on this, whereby identify theft can result in mixed up prescriptions, meaning that the victim patient might not be able to obtain the medication that they need.

Importantly, with much of the industry relying on OT, operational disruptions can impact the manufacturer's ability to supply patients with treatment and medication, thus potentially having fatal consequences. This was the case in the attack on Merck, whereby the company's ability to supply HPV vaccines was impacted.

HAC-1 Solution

Many times, enterprises' IT and security teams struggle in providing complete and accurate visibility into their hardware assets, especially in today's extremely challenging IT/OT/IoT environment.

This is due to the fact that often, there is a lack of visibility, which leads to a weakened policy enforcement of hardware access. This may result in security accidents, such as ransomware attacks, data leakage, etc.

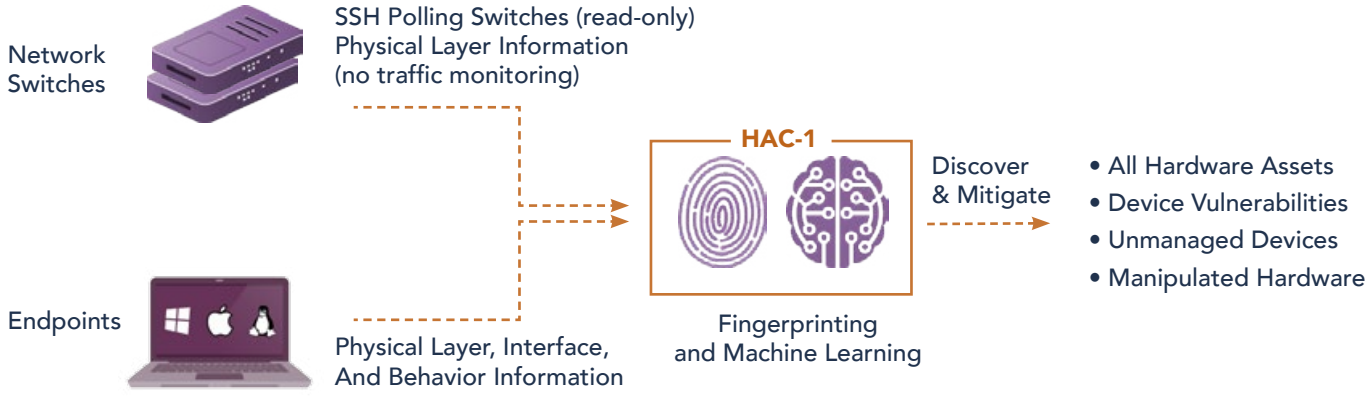
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them, as well as take advantage of the "blind" spots – mainly through USB Human Interface Device (HID) emulating devices or Physical layer network implants.

In addition to the deep visibility layer, a comprehensive policy enforcement mechanism recommends on best practice policy and allows the administrator to define a strict, or more granular, set of rules for the system to enforce.

Sepio is the leader in the Rogue Device Mitigation (RDM) market and is disrupting the cybersecurity industry by uncovering hidden hardware attacks operating over network and USB interfaces. SepioPrime, which orchestrates Sepio's solution, identifies, detects and handles all peripherals; no device goes unmanaged.

The only company in the world to undertake Physical Layer fingerprinting, Sepio calculates a digital fingerprint using the device descriptors of all connected peripherals and compares them against a known set of malicious devices, automatically blocking any attacks. With Machine Learning, the software analyses device behavior to identify abnormalities, such as a mouse acting as a keyboard.

How It Works



HAC-1 - Visibility & Security of Hardware Assets

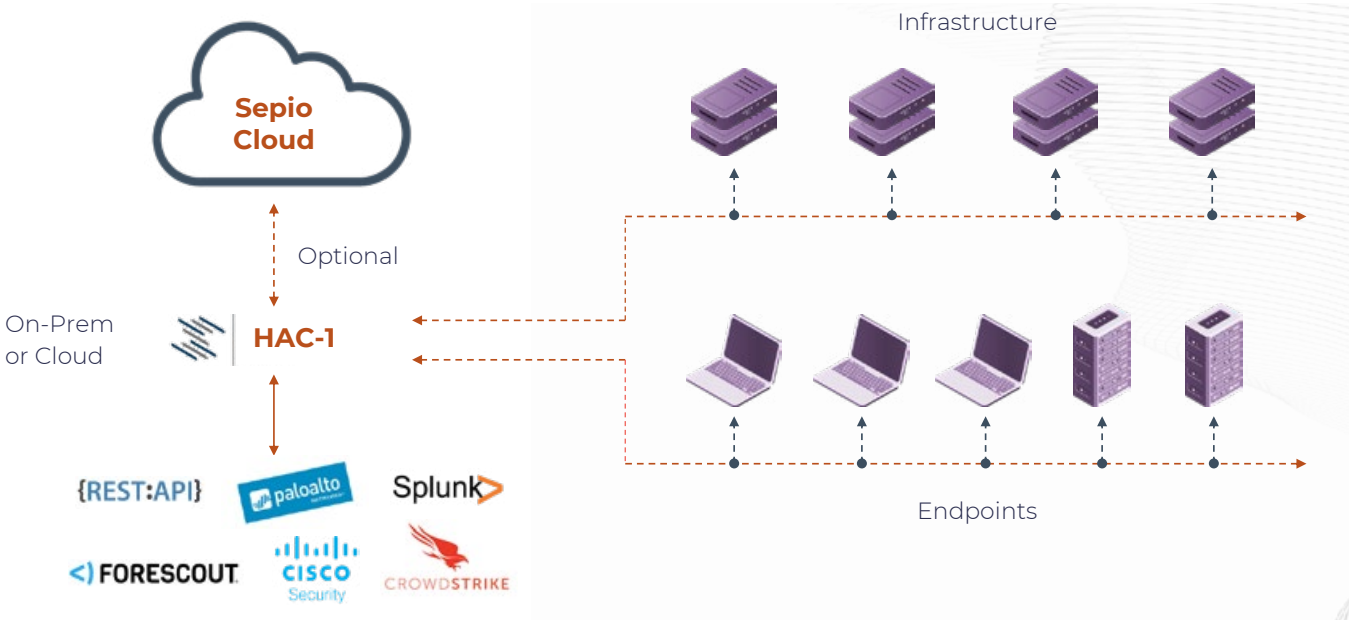
Main Benefits

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.

System Architecture



LEARN MORE

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.

SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS