SEPIO

EBOOK

12 Ways to Lower Your Cyber Physical Risks When Working Remotely

KEY FINDINGS

- 70% of people work remotely at least once a week.
- 53% of people work remotely for at least half of the week.
- Careless/uninformed staff cause 25% of all cyberattacks.
- Rogue Devices are becoming an increasingly popular attack tool.
- A work Remote Work Policy is essential.
- Company-issued devices will be more beneficial for organisations.
- Rogue Device Mitigation is imperative.

> **BYOD Enterprises have shifted to BYOO – Bring-Your-Own-Office.**

INTRODUCTION

Working remotely is becoming increasingly common not only due to the many benefits it brings employees and employers but, with globalisation, employees are often travelling all over the world and thus are not always physically in the office. Today, 70% of people, globally, work remotely at least once a week and 53% work remotely for at least half of the week. Due to the circumstances of the global pandemic that is COVID-19, the portion of the population that are still working in non-essential services are working remotely. Working remotely is essentially working anywhere but the office and it can mean using one's own personal device for work purposes – known as BYOD (Bring Your Own Device) – or having company-issued devices that may, or may not, be used for personal purposes. However, risks multiply when remote users hook up non-company monitors, printers, and other peripherals to devices connected to the company's network; be that company-issued or personally owned.

Spoofed peripherals and network implants – both of which are known as Rogue Devices – are increasingly becoming the weapon of choice for bad actors. These Rogue Devices have the ability to disseminate various forms of malware, perform man-in-the-middle (MiTM) attacks, advanced persistent threat (APT) attacks, network sniffing – including keylogging – and, importantly, data breaches. The consequences can be perilous and can last for a number of years after the attack itself is carried out.

Rogue Devices, besides carrying out noxious attacks, are almost impossible to detect, thus making them extremely threatening. Spoofed peripherals, such as manipulated USB devices, are recognised as legitimate human interface devices (HIDs). Network implants, on the other hand, go completely undetected as they operate on Layer 1 – the Physical Layer – which is not covered by existing security software solutions. As such, Rogue Devices do not raise any alarms.

Awareness is vital when aiming to reduce the risk of these attacks occurring. However, these attacks, although becoming more frequent, are less publicised and therefore even staff that do have cybersecurity training might not be aware about hardware attacks.

Any organisation in any sector can be a target, including:

- Critical Infrastructure.
- Data Centres.
- Telecoms.
- Financial Institutions.
- Healthcare Facilities.
- Hospitality.
- Retail.
- Government Agencies.

RISKS

Data

Working remotely often means employees have a significant amount of company data on their devices and can, therefore, be the target of an attack. Around 50% of businesses worldwide are concerned about employees inappropriately sharing company data via the personal devices they use for work purposes. Moreover, 54% of businesses have had data exposed because employees have lost devices that obtain sensitive information. Lost devices present a serious security risk; hackers have no problem circumventing passwords and have even utilized Rogue Devices to bypass biometric authentication. Since 65% of organizations cannot wipe devices remotely, the data on a stolen or lost device is easily accessible to a bad actor that has gained access to that device.

Working remotely often requires information to be shared. Should employees being working on a public WiFi hotspot, the information is being disseminated over an unsecured network. Remote Desktop Access is a common feature of remote work, and this can be risky as even if the individual is working on a secure, private network, those he is sharing the desktop with – which contains sensitive information – might not be, and the router to which they are connected to might have been compromised. Data is the most important aspect of working remotely as it means malicious actors can cause damage to an organisation without ever gaining physical access to its premises.

Insufficient Security

Depending on the organisation's policy, when working remotely employees might be permitted to use their personal devices (BYOD). However, personal devices will not have sufficient security as it will hinder the user's personal experience. Any security measurements a personal device has will not be suitable to protect against corporate data breaches or network intrusion, whereby an attacker can move laterally through the organisation's network and exploit further vulnerabilities. As such, personal devices are an appealing attack target, demonstrated by the fact that 50% of companies that allowed BYOD were breached by an employee-owned device. Moreover, using personal devices means security feature disparities, thus impacting capabilities.

Personal devices often have poor authentication since substantial authentication measures can act as a hindrance when being used for non-work-related purposes. They might only have single-factor authentication which most likely will be a password, and this is a serious risk to organisations. Even if devices have biometric authentication features, a password is almost always in place as an alternative. Passwords are easy to crack for hackers, and Rogue Devices can aid in this by keylogging to gain logon credentials, as well as being able to bypass biometric authentication.

> **"As a CISO you no longer have control of what is being connected to your employee's end-point"**

Employee Action

Careless/uninformed staff cause a quarter of all cybersecurity attacks and working remotely only increases the chances of this happening. Employees have no idea what is being connected to their device at any time, and they have no ability to control that. People might buy the cheapest or nicest looking device online, which is actually a Rogue Device, and plug it into their device completely ignorantly. Furthermore, employees working remotely in foreign countries are exposed to a novel environment meaning they are even less familiar with what they are plugging into their device.

Connecting to a public WiFi hotspot is common when working remotely, yet highly risky as the router might have been compromised with a network implant, thus allowing the perpetrator to gain remote access to, and manipulate, the data on the network and connected devices. Similarly, naively using public charging kiosks is hazardous as these chargers, too, may have been manipulated.

Employees can very easily fall victim to social engineering attacks. Should "someone" approach an employee working remotely and offer a charger, that charger can provide that "someone", who is actually a bad actor, with remote access to the company's sensitive information and data. Likewise, offering gifts, such as manipulated USB devices, is an easy way for an attacker to have their victim use a Rogue Device.

Malicious employees pose a grave danger to organisations, especially when working remotely as there are no prying eyes to catch them out. These ill-intentioned employees might make use of a Rogue Device to carry out their attack.

WAYS TO LOWER THE RISKS

1 > Remote Work Policy

The first thing that needs to be done is to establish a Remote Work Policy that clearly defines how employees can work remotely; whether that means defining a BYOD policy, or requiring employees to use company-issued devices only, in addition to determining the extent to which staff can carry out their jobs with minimal restrictions, if any. The Remote Work Policy should be approved by a range of stakeholders to ensure it is based on the interests of all parties involved with the company as to certify efficiency. The following risk reducing procedures might be included in the provisions of the Policy.

2 > Principle of Least Privilege

This gives employees access to only the data they need to perform their job, thereby reducing the amount of data on employees' devices. Since the exposure of data is one of the greatest risks when working remotely, the Principle of Least Privilege reduces the amount of data being purloined, should an attack take place.

3 > Zero Trust Network Access

Based on the principle of "never trust, always verify", ZTNA ensures that trust is not automatically given, and that access is granted on a "need-to-know", least-privileged basis, defined by granular policies. ZTNA, as such, recognises that trust is a vulnerability and therefore prevents lateral movements; the prime technique used by malicious actors as their point of access is usually not their actual target. ZTNA therefore complicates and incommodes the attack.

4 > Updated Anti-Malware Software

Although a Rogue Device will not raise alarms, it might install malware and, if the malware is known to anti-malware software, this will be detected. For the malware to be detected, the organisation's anti-malware software must be up to date to ensure the most comprehensive coverage for known malware.

5 > Virtual Private Network

VPNs create encrypted "tunnels" between a user's device and the internet. Employees can access their files remotely without being "watched" as no-one between the user and the server they are connecting to can gain access to the

data that is being transmitted, thus providing greater protection from network implants. VPNs are crucial when working remotely as, when connecting to a public WiFi network, one can never be sure who set it up or who else is connecting to it.

6 > Patch Vulnerabilities

Working remotely means risk of a cyberattack, therefore it is imperative that vulnerabilities are patched so that bad actors cannot exploit them. Perpetrators of an attack primarily seek to exploit vulnerabilities and, should they succeed in infiltrating the organisation's network, can move laterally to identify more. Identifying and patching vulnerabilities is a vital procedure. Before deploying the patch, however, an assessment should be conducted to ensure its efficacy and to determine that it will not introduce any new types of risks.

7 > Improved Authentication

Biometric authentication is the most secure form of authentication and should be used whenever possible, be that fingerprint or facial recognition, which most devices come imbedded with. The importance of using all native security features of a device must be emphasised by the organisation, as well as always locking the device whenever it is not in use.
Ideally, multi-factor authentication will be most beneficial, with phone-as-a-token being most useful when working remotely.

8 > Remote Wiping

Lost or stolen devices can pose a challenging risk to an organisation as a malicious actor can easily access the data on it. Enforcing a policy that allows remote wiping of the device will be highly favourable as it will mean that there will be no valuable information on the device for the hacker to exploit. Importantly, the wiped data should be remotely backed up to prevent unrecoverable damages.

9 > Containerisation

For organisations that permit their employees to use personal devices when working remotely, containerisation is a suitable way to ensure enhanced security. Containerisation segregates a portion of the device into its own protected bubble which requires password access, thus isolating and regulating – with a separate set of policies – specific files, folders and applications.

10 > Staff Education and Training

One of the most vital ways to reduce cyber risks is to enhance employee's education and training on the topic. Social engineering, for example, can only be prevented by increased training and awareness. Organisations need to stress the risks of connecting peripherals to their devices and make them suspicious of where the peripheral is coming from. Peripherals should always be bought from reputable sources such as Apple. Carrying a portable charger when working in locations other than one's home will ensure that employees are using a trusted peripheral. Furthermore, employees should know not to let others use the device they use for work purposes.

11 > Company-Issued Devices

This allows the company to be in full control over what security measures are enforced and can guarantee that the measures level up to their expectations. Furthermore, issuing uniform devices will ensure that there is consistency in terms of security features and capabilities. Company-issued devices might be explicitly used for work purposes only and organisations can implement security features that ensure this, such as whitelisting, application installation control and mobile device management. Additionally, extra security measures can be imbedded such as data encryption and antivirus software. In some cases, company-issued devices will prohibit peripherals from being used altogether – besides those that have been pre-defined – thereby reducing the risk of a manipulated USB from being used (the ones that have been permitted can still be compromised).

12 > Rogue Device Mitigation Software

The best way to reduce the risk of Rogue Device attacks is to implement a Rogue Device Mitigation software that can detect such attack tools and take action to prevent their success. Sepio offers such a software that protects both the endpoint and the network.

> **“While your Enterprise shifts to Work-From-Home you need to make sure that the assets left in your site are well protected.”**

HAC-1 SOLUTION

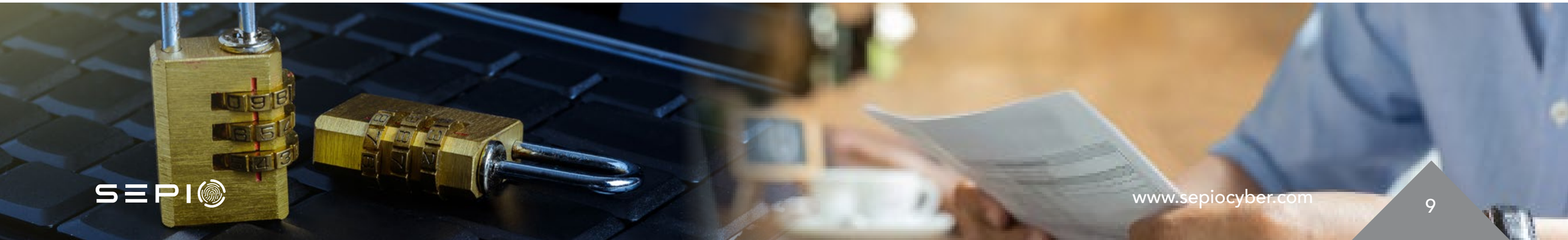
Many times, enterprises' IT and security teams struggle in providing complete and accurate visibility into their hardware assets, especially in today's extremely challenging IT/OT/IoT environment. This is due to the fact that often, there is a lack of visibility, which leads to a weakened policy enforcement 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.



HAC-1 - VISIBILITY & SECURITY OF HARDWARE ASSETS

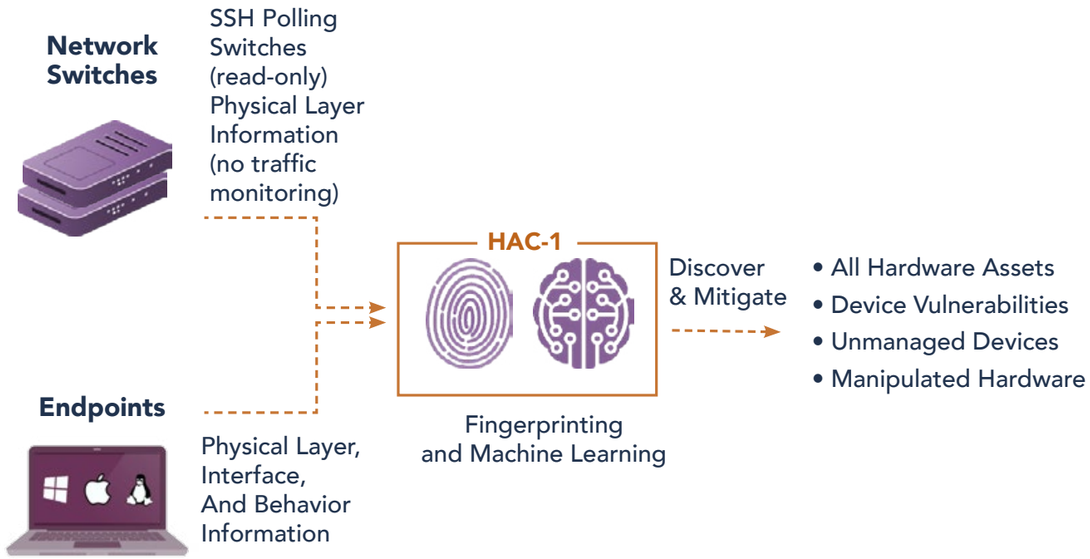
Main Benefits:

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.

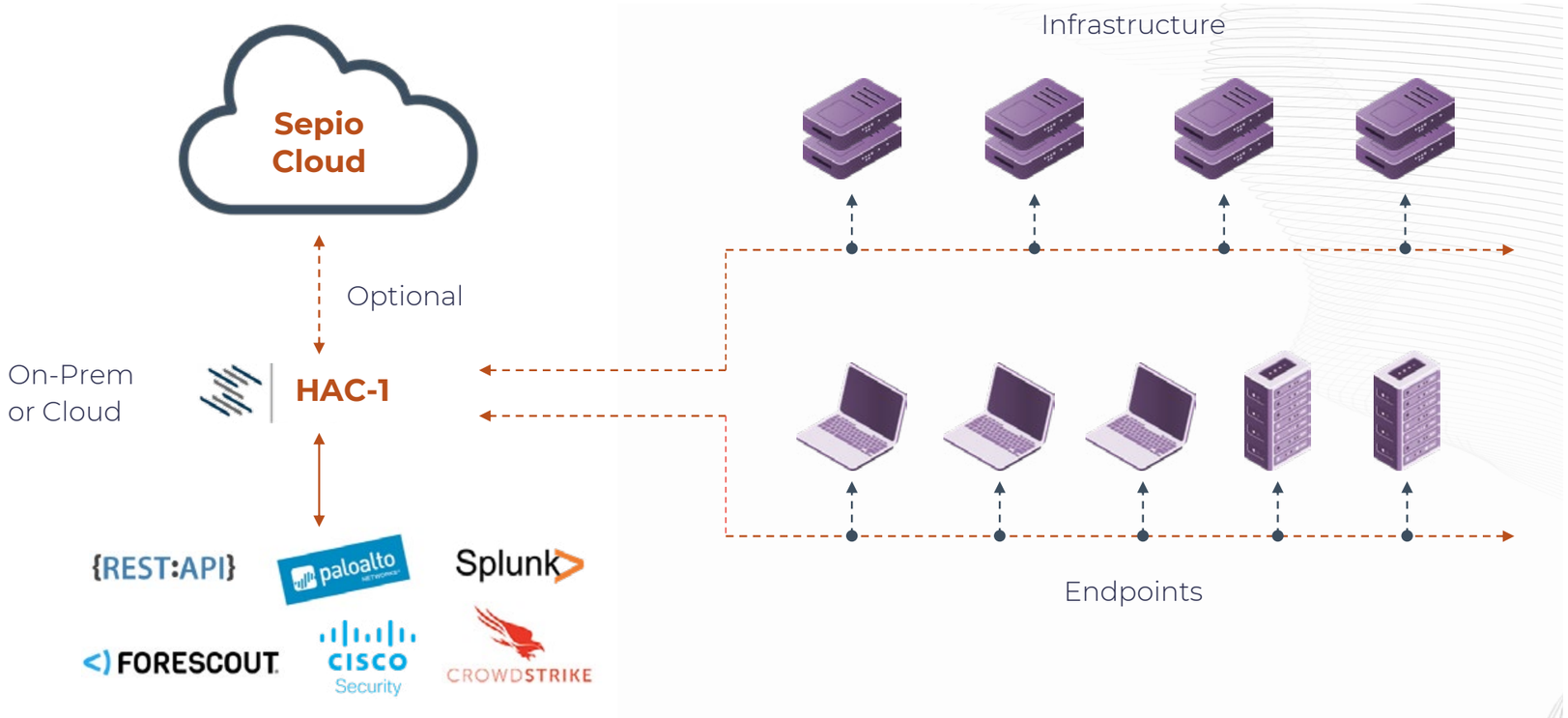
Full Control through Predefined Policies: Enterprise-wide policies enable compliance, regulation and best practices. With predefined templates and no baselining or whitelisting, and no requirement for a clean environment start, Sepio provides a fast and easy setup.

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.

How It Works



System Architecture



We are also available on:

Linkedin >>
https://www.linkedin.com/company/sepio-systems/

Facebook >>
https://www.facebook.com/cybersepiosystems/

Twitter >>
https://twitter.com/sepiosys

<< LEARN MORE >>