BYOD Risks

PROBLEMS AND SOLUTIONS

A Sepio white paper

SEPIO

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

Contents

INTRODUCTION

Bring Your Own Device (BYOD) is a trend whereby employee-owned devices are being used within a business. BYOD policies enable employees to use the same devices for personal and office use, allowing them to work remotely if need be. This is a trend that is growing rapidly due to the myriad of benefits it provides both the business and the employee. As of 2015, 82% of organizations are accepting the use of personal devices for work-related purposes, and the BYOD market is estimated to increase by 15% every year until 2022, from a starting value of $30 billion in 2014.

The corporate world has three key approaches for allowing their employees to operate mobile devices internally, and externally, for work-related purposes.

BYOD (Bring Your Own Device)

This is what will be explored in this white paper and it involves businesses relying on their employees to utilize their own devices, such as mobile phones, laptops and tablets.

COPE (Company Owned, Personally Enabled)

In this case, the company issues secured mobile devices to employees which can be used for personal and work purposes. A key fault with COPE is it restricts the employee to use a specific platform and operating system which might be disliked, therefore encouraging them to revert to using their own mobile devices. It can also be invasive to employees' privacy as the company's IT department can observe all actions an employee makes on their device.

CYOD (Choose Your Own Device)

This is a compromise between COPE and BYOD whereby the company will provide employees with a list of previously approved devices that can be used. The devices come pre-installed with business software and security, but ultimately the device belongs to the employee. Again, however, this still prohibits complete freedom for the employee.

"82% of organizations are accepting the use of personal devices for work related purposes"

ADVANTAGES

COST REDUCTION

Primarily, BYOD alleviates costs for the organization as funds do not need to be spent on providing equipment for employees. According to Staffbase, employers can save more than $1,000 per employee with BYOD policies. This is a significant advantage to an organization of any size and is an attractive feature of BYOD.

BYOD saves employers over $1,000 per employee

EMPLOYEE BENEFITS

BYOD promotes workplace flexibility, which is a key selling point to prospective employees, especially millennials, who are often highly employable. As such, loyalty, morale and employee engagement increase when the workplace is more flexible.

Moreover, around 80% of employees believe that managing a single mobile device helps them balance their personal and professional lives. Again, this results in higher productivity as work can be accessed anytime and anywhere, without needing to be in the office.

A more balanced personal and professional life felt by 80% of employees

SATISFACTION

Workplace flexibility and, as a result, a more balanced personal life, affords employees with greater job satisfaction. This serves the organization as satisfied employees will be more productive and more engaged in their work, resulting in higher levels of efficiency.

INCREASED PRODUCTIVITY

Companies avail from higher productivity, with over 50% of employees feeling more productive when using their own devices at work. As BYOD allows employees to work remotely, absence from the office due to bad weather or doctor's appointments, for example, will not hinder productivity since employees can work outside the office. Likewise, employees with lengthy commutes can work from home a few times a week, thereby increasing their efficiency rather than wasting time getting to and from the office.

"Employee Satisfaction" and Productivity are the prime benefits to **58%** of surveyed employees.

DISADVANTAGES

COSTS FOR EMPLOYEES

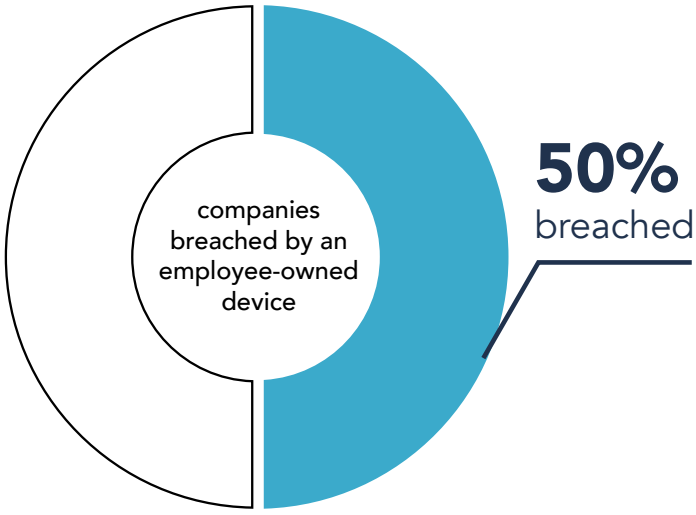
Using their own device suggests that employees will supply themselves with devices, thereby incurring the cost. Additionally, repair costs to these devices will fall on the employee, some of which can be substantial.

DEVICE DISPARITIES

Different devices have ranging operating systems and, as such, various capabilities. This leads to inconsistencies among employees' abilities due to the ranging functionalities of the devices being used. In certain cases, some devices might not even be adequate to carry out specific tasks. Additionally, devices are of different quality, leading to the same problem of inconsistency.

SECURITY

The greatest weakness of BYOD is the security risks that come with it. For the 26% of Tech Pro Research's survey respondents who have not adopted – nor are planning to – BYOD, security concerns were the most common reason as to why. Employee devices will not have the same security measurements that an organization's device will have, and any security measurements a personal device has will not be suitable to protect against corporate data breaches or network intrusion. This is a grave threat demonstrated by the fact that 50% of companies that allowed BYOD were breached by an employee-owned device.



"Security concerns were the main reason for companies that did not implement BYOD."

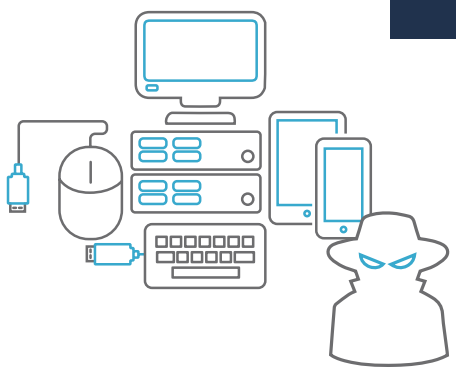
Employees can walk away with a significant amount of data on their devices and can, therefore, be targets for attacks. These attacks can occur when an employee uses their device remotely and connects to a public WiFi hotspot whereby a hacker can infiltrate the device. Similarly, using public charging kiosks that have been manipulated allows a perpetrator to gain remote access to the device. Social engineering attacks also present a risk. Should "someone" approach an employee looking distressed and say "Hey, my phone has been stolen, can I borrow yours to make a call?", that "someone", who is actually a bad actor, can use the employee's phone to gain access to sensitive information and data.

Malware can get onto mobile devices numerous ways including through spam emails, links and rogue programs or apps. Similarly, trojan malware can be embedded through SMS messages and social network links. Spoofed peripherals also have the ability to inject malware onto the endpoint to which they are connected. Malware is perilous as it can spread to other devices on the business' network, generating considerable damage. US mobile malware rates are increasing by 75% each year, with Apple's operating system receiving five times more malware in 2015 than in the five years previous. These figures indicate a growing risk to organizations that permit BYOD.

Stealing or acquiring lost devices is an alternative way for hackers to access the organization's network and obtain valuable information. The best intrusion-detection system and anti-virus software will be futile if this happens. Password protected devices are not safe either as circumventing a password on a stolen/lost device is no challenge for a hacker.

Insiders also pose a threat to an organization and BYOD facilitates their operations. Mobile devices make it easier for malicious employees to access the company's network and pilfer sensitive data.

THE RISKS



OUT OF THE 70 MILLION DEVICES LOST OR STOLEN EACH YEAR

ONLY 7% WERE RECOVERED

15% *of employees have accessed sensitive data from non-work-sanctioned devices*

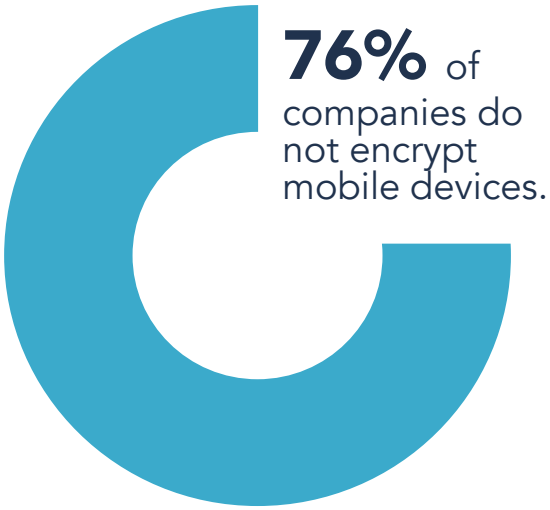
54% *of organizations don't include employee-owned devices in their backup plans*

65% *of companies cannot wipe devices remotely*

TECHNOLOGICAL SOLUTIONS

DATA ENCRYPTION

Encrypting data that goes beyond the control of the organization is necessary and it should be performed throughout the data's life cycle. 76% of companies do not encrypt mobile devices, which makes them extremely vulnerable. Furthermore, the IT department should take control of encryption keys to prevent unauthorized access and to maintain the encryption, should a breach transpire



APPLICATION INSTALLATION CONTROL

Some devices and operating systems can give control to the IT department over which applications are installed on an employee's device. iOS and Android operating systems provide this feature. Employees, however, may feel as though their freedom is being encroached.

MOBILE DEVICE MANAGEMENT

Mobile device management (MDM) is a solution that gives the organization the capacity to secure, monitor, manage and support mobile devices centrally by integrating them into a network. However, taking advantage of this could create a restrictive user experience for the employee.

CONTAINERIZATION

This is a method by which a portion of the device is segregated into its own protected bubble – separate from the other applications and content on the device – with password access required. This solution, similar to sandboxing, can isolate individual files, file folders, as well as entire applications and regulates them with a separate set of policies.

When logged into the containerized area, personal apps and other features that are not managed by the container are inaccessible. This is a more appealing solution to both the company and employees as it eliminates the possibility of accessing apps that do not meet the company's security policies when connected to the organization's network, but does not limit the employee from using the device how they want when not connected.

BLACKLISTING

This allows an organization to block apps and websites that are deemed as a security threat or those that might impede productivity, such as games and social networking apps. Additionally, file sharing services, such as GoogleDrive, can be blacklisted to preclude confidential information from being distributed.

WHITELISTING

The opposite of blacklisting, whitelisting gives employees access only to a list of approved applications. This can be a more appealing solution to employees as there is a more extensive range of applications and websites that exist. For IT departments there is less pressure to identify websites and applications that need to be specifically blacklisted making whitelisting a more secure solution.

ANTIVIRUS SOFTWARE

Installing antivirus software on individual devices will enhance security by protecting devices from malware attacks.

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.

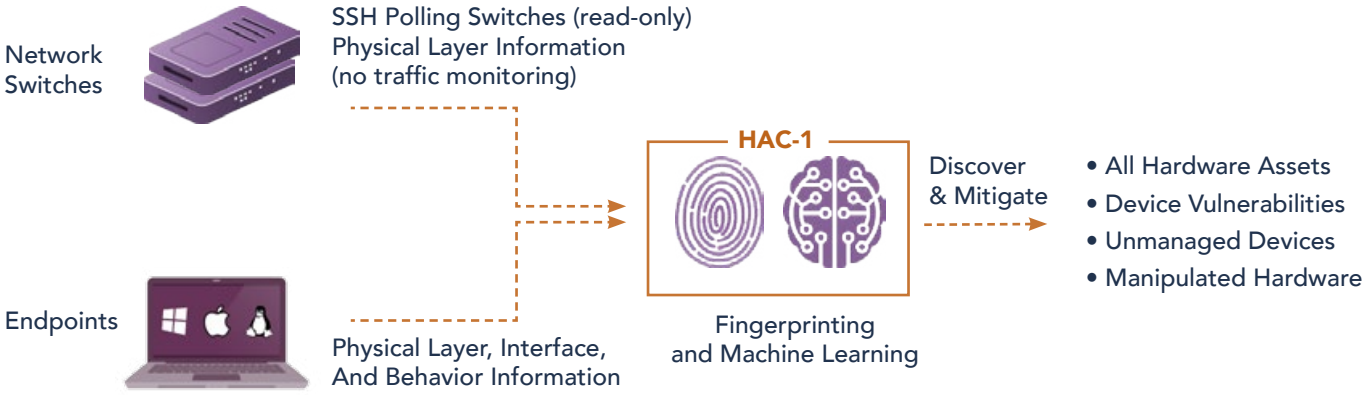
In order to address this challenge, ultimate visibility into your Hardware assets is required, regardless of their characteristics and the interface used for connection as attackers. Moreover, it is important to be practical and adjust to the dynamic Cyber security defenses put in place to block them, 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



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