Addressing PHI Security on BYOD (and COPE)

Contents

©2019 Actifile Ltd. All Rights Reserved.

https://www.actifile.com

Introduction to BYOD use in Healthcare

The trend to support employee chosen (or even employee bought) devices started with mobile devices. Many employees preferred to use their personal phone for business. For many it was preferable to lugging a corporate device alongside a personal one.

Technologies such as EMM and MDM allowed enterprises to keep corporate data secure and separated from the employee's personal data on the mobile devices, thus observing the privacy of employee data. This worked rather well (and is now a requirement under SOC II) but worked mainly in the areas of personal productivity like mail and calendar apps - because mobile devices are mostly used to view and read content - not to create or substantially modify it.

So naturally employees wanted to be able to create and modify data using their own choice of computer (usually a laptop). This coincided with the gig economy trend - offloading non-core corporate tasks to part-time employees and freelancers. These gig economy employees would also have their own laptops and desktops.

Glossary of BYOD terms

Type		**Ownership**	**Administration**	**TCO[1]**
COBO	Company Owned Business Only	Company	Company	++++
COPE	Company Owned Personal Enabled	Company	Employee is a local admin	++
CYOD	Choose Your Own Device	Company	Employee is a local admin	+
BYOD	Bring Your Own Device	Employee	Employee is a local admin	-

The BYOD Advantage (and Risk)

For both employers and employees, BYOD computers have many advantages. The cost of provisioning devices is lowered (or even eliminated). Employees can use the computer and software that works best for them and enhances their productivity. Freelancers can work part time. Consultants don't have to lug multiple provisioned devices.

But BYOD has one key disadvantage: it is an unmanaged asset.

As such, it can pose two main risks to the organization:

1. Data (e.g. PHI) abuse and loss risk
2. Introduction of malware into the organization

Enterprises provided laptops (COBO and some COPE) have a stack of cyber security systems that address these concerns: From endpoint DLP to prevent data loss, to EDR and AV to eliminate malware, to group policies to ensure passwords and connections are managed to enterprise standards. As many CISO and administrators discovered, using these tools with BYOD is challenging.

[1] TCO – The aggregate cost of device, security and business applications licensing, provisioning costs, maintenance, advanced replacement, etc.

BYOD, Healthcare and Data Loss Risk in Numbers

A recent study by HIMSS[2] , shows that the major user cases for BYOD in healthcare was accessing clinical information (using an application or retrieved from an electronic health record system). Another use was finding information (educational) as well as consulting with other caregivers. Doctors sometimes provide care under more than one system provider (e.g. in private practice as well as a hospital or clinic) BYOD allows them to carry one device that gives them access to all of their patient data. Similarly, nurses may provide care as contractors for home care providers. Using a BYOD allows these nurses to carry one device that provides access to records for the patients under their care.

The use of BYOD is widely adopted in the healthcare industry: a 2015 study published in the Journal of Hospital Librarianship estimated that 85 percent of healthcare professionals were bringing their own devices to work. And, according to a HIMSS analytics study, almost 40% of the healthcare professionals use a laptop. Further to that, a HIPAA Journal study shows, that about 60% of data loss were due to lost or stolen computer (31%) or employee error (29%). In fact, only 8% of data loss was attributed to a malicious insider. So strong protection of the PHI data on endpoints, should mitigate most of the risk associated with a BYOD policy.

As an example, in one rather egregious example, a laptop containing 400,000 PHI records was stolen from a parked car. That means that ensuring that data is inaccessible on a lost/stolen/discarded computer, coupled with controls that limit damage due to errors will go a long way to demonstrating responsibility with PHI. [3]

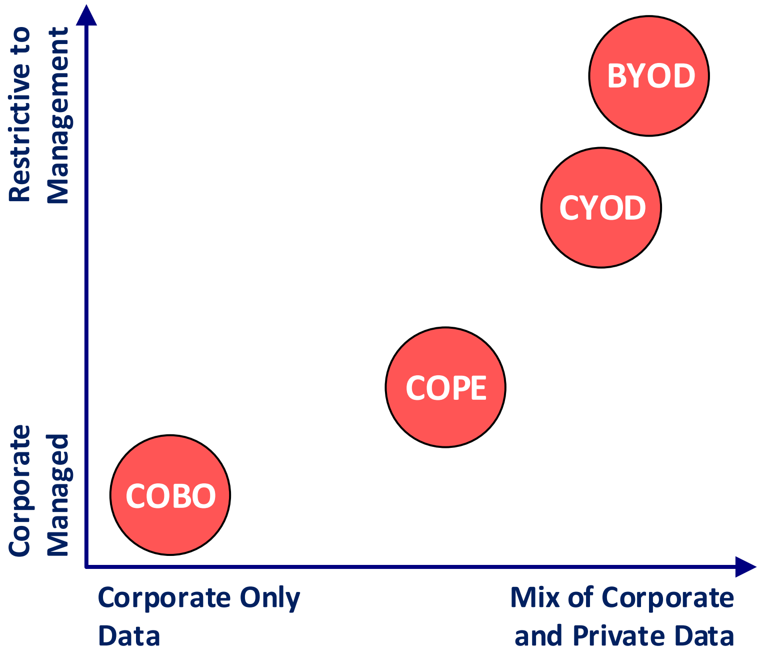
[2] Source - https://www.himssanalytics.org/sites/himssanalytics/files/2017_Essentials%20Brief_Mobile_SNAPSHOT%20REPORT.pdf

[3] Source - https://www.hipaajournal.com/healthcare-data-breach-statistics/

From COBO to BYOD: The Evolution to Mixed Use Devices

As organizations move more of their essential business operation to Gig economy employees, more regulated and confidential data is downloaded to BYOD endpoints. Cloud has enabled much of this process as there is no longer any need to connect to a VPN and simply onboarding a user enables them to access corporate resources (like EMR systems) from their home computers or laptops.

The implications of BYOD vs. COBO are substantial. Looking at the graph below analyzes the trajectory of BYOD adoption:



From the standard corporate provided and corporate managed COBO, where any data found is considered to be the property of the organization (personal use is usually discouraged). And where therefore, the organization is free to install any (and all) security applications needed to manage and secure the data.

Through COPE, where the employer buys and provisions the device, but the employee is free to use the device for their personal use. The mix of personal and corporate data requires care in the use of security applications – so as not to expose employee data.

For BYOD and CYOD, where the employee acquires the device, the mix or private and corporate data is thorough and security applications which compromise privacy can no longer be used. The main difference between them is that for CYOD the employer provides the employee with a stipend for the device.

Challenges to Securing Data on BYOD and COPE Laptops

Striking a balance between securing PHI (and other corporate data), employee productivity, TCO, and employee privacy is critical to ensure BYOD is to be a tenable solution. Furthermore, any controls used must be easy to deploy and manage by the employee.

Challenge	**Description**
Securing PHI and other sensitive data	Enabling BYOD necessarily means that employees get access to data stored in the cloud or in corporate resources. Some of this data can be accessed and used online, but some can and may be downloaded to the end point. Securing this data against theft or abuse is important. Furthermore, this data may consist of customer records, patient records, PII, PHI or any other privacy and business sensitive nature. Regulatory compliance may also be required.
Respecting the employee's privacy	Since this is the employee's personal laptop (or being used for personal use as a COPE device), it is likely to store the employee's (and their family) private data as well as data related to their personal interests. If the employee is a contractor or a part-time employee, the laptop may also contain information owned by the employee's other employers. Obviously, security applications that do not infringe on the users' privacy are needed. For some, it may be a matter of configuration. For other, a different approach may be needed.
Policy compliance	Organizational security policies such as password policies, utilizing AV (and other endpoint security) applications, full disk encryption, MFA (multi-factor authentication), archiving, etc. may be difficult to enforce on a BYOD. In some cases (like cell phones) an MDM or EMM may help. But a different approach is needed for laptops and external computers.
Addressing Ransomware	Ransomware is a newer concern for many security managers. If an employee's device is locked by an activated ransomware, it may become impossible to access any data which was updated or captured on the devices. Which makes it important to archive sensitive PHI on the fly (so that if ransomware is activated, no PHI is lost).

The Cyber Security Eco-system: Alternative Approaches to Securing Data at the Endpoint

As we stated above, there are two main issues that enterprises have to contend with: (i) Data abuse and loss risks and (ii) introduction of malware onto the device and potentially into the network.

Options for the latter that do not compromise privacy include systems such as CASB (and other cloud AV and gateway systems) and, for the endpoint, AV and EDR. Care must be taken to quarantine any detected file on the users' endpoint (rather than uploading to a corporate quarantine) as the file may include non-corporate information.

For the former, the task is harder. Some, like rights management systems (RMS - E.g. Microsoft WIP) and Virtual Desktops (VDI - E.g. Citrix) can provide some protection at a large cost of overhead and usability. Creating the rules required for RMS is a daunting task for an employee. Deciding on a global rule set to automate the protection is even harder. Also, RMS typically do not work well with cloud systems and require integration with cloud systems to function. Making their deployment both expensive and risky.

For VDI the main issue is connectivity: A reasonably fast connection is necessary. Some organizations can make it work - e.g. large insurance companies that have a designated "consultant area" with high performance networking. They don't expect these consultants to work from home. But for many (e.g. Doctors) performance can be spotty at different areas of their work and trying to get medical records while doing doctor rounds is frustrating.

Data loss focused systems (such as DLP) cannot be used at all. While they are very good at detecting information on the endpoint, they cannot differentiate corporate-owned and non-corporate information. The result is that the DLP system will detect and react to all data on the endpoint enforcing corporate rules on it. System reports will contain both corporate as well an employee personal information - a liability for the organization.

Can data security policies bridge some of the gaps? Even with substantial investment in training, not every BYOD carrying employee will install a corporate level password, nor keep an AV updated on their machine.

For BYOD a separate data centric security policy is needed. To back it up, isolation of the corporate-owned information from any other information on the endpoint is the only way to secure the data without compromising security, privacy and efficiency.

PHI Isolation: Actifile's Answer to Securing PHI on BYOD and COPE

Actifile's data security endpoint was built from the ground up to address the problems associated with BYOD usage. Built as an easy to deploy app managed from the cloud, Actifile's main functionality is to keep PHI and other corporate data separate from the employee's data. By providing isolation, DLP and control activities can be focused on PHI and other corporate data without compromising the employee's privacy.

Challenge	How Actifile Addresses the Need
Securing PHI and other sensitive data	Actifile keeps track of sources such as EMR and EHR systems and tracks data retrieved from those sources. Furthermore, it is a simple setting to encrypt the data retrieved from these sources, transparently. So that if the computer is lost or stolen the data is safe and secure. A remote wipe ability ensures that when an employee leaves, the health provider can remove the PHI from their laptop.
Respecting the employee's privacy	Since Actifile tracks the data gleaned from organizational sources (e.g. EMR and EHR, or applications like the corporate email), the system does not access nor track the employee's data. Nor does the system track or in any way access information owned by other employers.
Policy compliance	Actifile can provide access password to stored PHI (so that even without a machine password the data is inaccessible without a purpose login). Furthermore, Actifile can report on the availability of an AV (or other policy required infrastructure).
Addressing Ransomware	Ransomware is a newer concern for many security managers. If an employee's device is locked by an activated ransomware, it may become impossible to access any data which was updated or captured on the devices. Which makes it important to archive sensitive PHI on the fly (so that if ransomware is activated, no PHI is lost).

Example Healthcare Use Cases

Visiting nurse services (Home Care)

What do they need to protect: PHI

Source of data: EMR and EHR systems

Devices: BYOD laptops used by home care professionals

Scenario: Home care professionals access the EMR systems to retrieve health records and other PHI which they download to their laptops. Even with substantial investment in training, not every BYOD carrying employee installed a corporate level password, nor kept an AV updated on their machine. The alternative to Actifile was to acquire laptops for the home care professional, an expensive ordeal indeed!

Actifile's Solution: Using source classification, all PHI information that is gleaned from the provider's EMR system is considered as patient sensitive data. The data is stored encrypted and an access password is enforced so that even when used on a laptop that doesn't have a system password, the PHI is protected.

Community Hospital

What do they need to protect: PHI and PII (health records and payment information)

Source of data: Various systems

Devices: Laptops (mainly administrators)

Scenario: Hospital administration uses various laptops to help them provide services efficiently. These laptops are used routinely to download medical records and payment records to resolve billing and healthcare issues. These records may remain on the device for a short or longer timeframe, creating unnecessary risk to PHI and PII.

Actifile Solution: Making use of Actifile's endpoint discovery component, files that contain PHI and/or PII are logged, tracked and encrypted to ensure they are all secure. Since the laptops used are owned by the hospital (COPE), employee privacy is treated as much of a concern as patient PHI and thus all detected information is treated as classified.

About Actifile

Actifile was founded by a team of Enterprise IT veterans who previously took cyber security and compliance startups to market success. The founders realized that networks are changing. Employees working on corporate controlled machines, connected to LAN’s protected behind firewalls are becoming the minority:

1. Endpoints are mixing business use with personal use. BYOD or even giving a user administrative permissions or access to websites is enough for the device to become mixed use.
2. Business applications are moving to the cloud. New organizations hardly have a data center while established ones are migrating to the cloud. Employees need of firewalled LANs is becoming rare.
3. Gig economy and remote employees. Many organizations are going global making it easier and more cost effective to find good workers. These employees are not subject to the rigors of IT.

Actifile was founded to address these issues. The Actifile product was designed from the ground up to address the problem of data loss from unmanaged endpoints (e.g. BYOD, CYOD and COPE).

For more information or a free consultation please check https://www.actifile.com or contact us at info@actifile.com.

©2019 Actifile Ltd. All Rights Reserved.