SECURE.SYSTEMS
WHITEPAPER

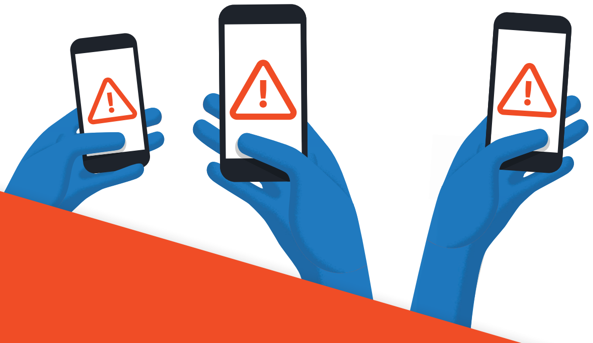
BYOD Will be One of Your Biggest Threat Vectors in the Next 12 Months – Here are 5 tips to reduce BYOD Risk in Your Enterprise

The IT cost savings from BYOD is undeniable, but the potential revenue loss and damage to your brand from cyber-breach is your greatest threat. This paper reviews how BYOD is fueling the fire for endpoint data risk and what you can do to reduce that risk.

To many professionals, mobile devices allow them to do their job more effectively. In law enforcement, mobility allows for a more efficient work flow of evidence logging, and in healthcare, physicians can provide faster consultations to patients at the point of care by using personal devices to perform professional searches. While these are just two examples of mobility in the modern workplace, employees across industries are using mobility to facilitate their day to day functions on the job. Because of the familiarity employees have with their own devices, Bring Your Own Device (BYOD) in the workplace is growing.

According to a TechPro Research Report titled “BYOD, Wearables and IoT: Strategies, Security, Satisfaction” the majority of the 206 employers (59 percent with 13 percent anticipating the adoption of BYOD in the future) surveyed allow employees to use personal devices for work purposes, connecting personal devices to company networks and data.[1] Many employers making the change to allow BYOD have years of experience using Enterprise Mobility Management and experience this growth comfortably.

While employees play an important role in influencing the adoption of the same mobile technologies that they’ve become accustomed to in their lives outside the office, employers also have their own incentives. An improved image, the possibility of cost-savings, and a more empowered staff all contribute to the desire of hospital networks and healthcare practices to make mobile devices available at the point of care. Organizations have two choices for accomplishing this goal: they can provide employees with mobile devices, or they can implement bring your own device (BYOD) policies.



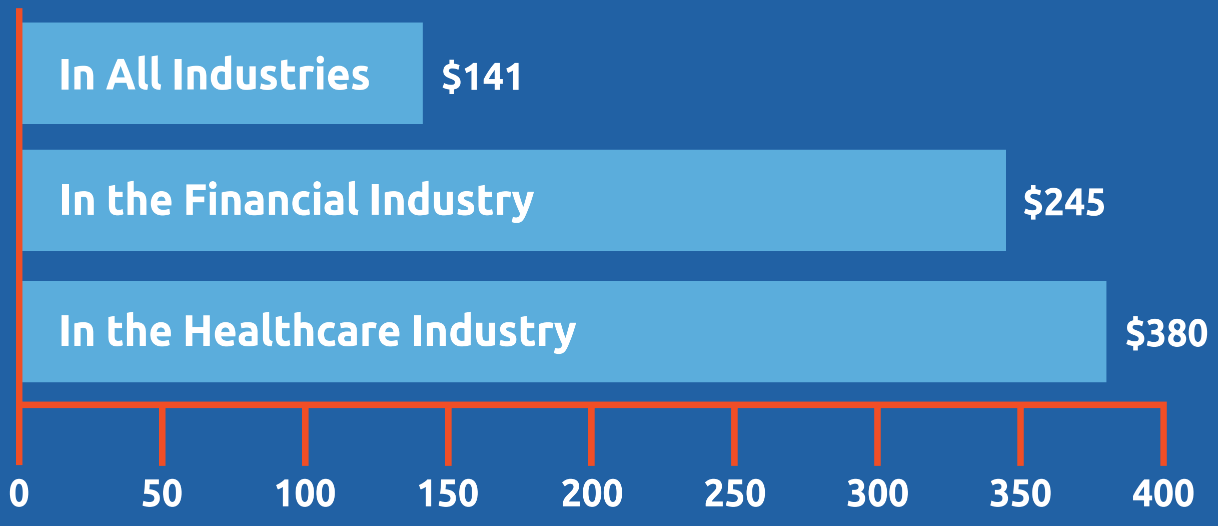
> “We don’t use mobile device security because too many other things are bigger issues; we haven’t yet experienced a problem with mobile security to cause it to be a higher priority.”

There are two primary motivations behind the BYOD approach: the convenience for employees of using a single device they’re familiar with, and the cost-savings organizations enjoy by not having to invest in hardware while improving worker productivity. However, despite the widespread adoption of BYOD policies, the Ponemon Institute report adds that more than half of organizations lack confidence in the security of employee-owned devices, and they’re right to feel that way.[2]

[1] http://www.techproresearch.com/downloads/research-byod-wearables-and-iot/

[2] https://www.ponemon.org/local/upload/file/ID%20ExpertsPatient%20Privacy%20%26%20Data%20Security%20Report%20FINAL1-1.pdf

The Average Cost of Lost or Stolen Data per Record in 2016



From the 2017 Ponemon Cost of Data Breach Study

As stated in Gartner's report, "Capturing Business Value from Mass-Market Mobile Technologies," "The mass-market mobile devices that are flooding most enterprises were not designed with security and manageability in mind... New ways to communicate and collaborate come with new ways to lose data, trade secrets and private information. In short, enthusiasm for mobile deployments has far outpaced mobile security."[3] Organizations may be worried about the security of employee devices, but that fear hasn't been significant enough to incite many of them into action. The reality is we just don't read about mobile device breaches in the news enough for mobile security to be front facing in enterprise computing.

The most recent Ponemon Institute Cost of Data Breach study reports that in 2016 the average cost of lost or stolen record was $141. The healthcare industry saw the most expensive loss at $380 per lost or stolen record, with financial industries next in line at $245 per record.[4] The difference in cost is important to note since healthcare data contains the robust content that cyber thieves want with PII and banking information all contained within in the same record.

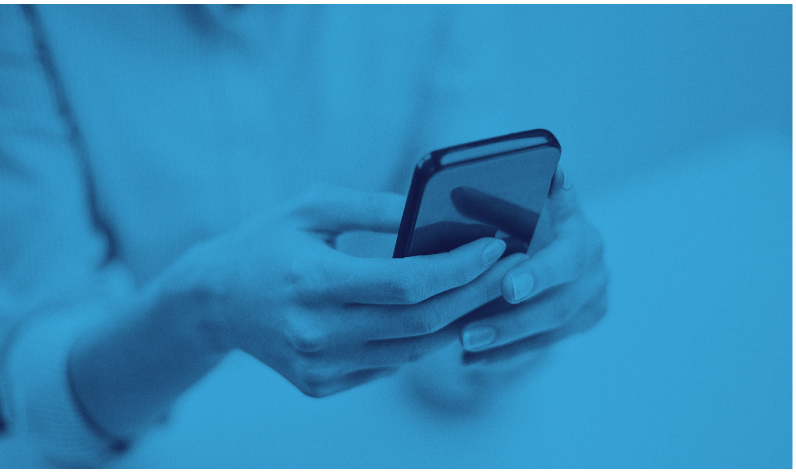
Without top-down initiatives to improve enterprise security practices, mobile security initiatives are inevitably put on the backburner while IT professionals move from project to project putting out other, seemingly more pressing fires. The Spiceworks survey "Weathering the Mobile Storm" illustrates that, despite virtually unanimous concern (98 percent) among security professionals about the risks associated with mobile devices, the general consensus can be summated from one InfoSec pro's response: "We don't use mobile device security because too many other things are bigger issues; we haven't yet experienced a problem with mobile security to cause it to be a higher priority."[5]

The reality is that information security professionals have to prioritize. According to the Information Systems Audit and Control Association (ISACA), the global shortage of cybersecurity professionals is expected to reach 2 million by 2019.[6] The group's "State of Cybersecurity" survey found that more than half of organizations took between 3 and 6 months to fill a security position, and a staggering 84 percent believe that fewer than half of the job applicants are actually qualified.[7] Meanwhile, almost 90 percent of consumers

[3] https://www.gartner.com/doc/1779628/executive-summary-capturing-business-value
[4] https://www.ibm.com/security/data-breach
[5] https://www.slideshare.net/SpiceWired/weathering-mobilestormreportoctober2014
[6] https://image-store.slidesharecdn.com/be4eaf1a-eea6-4b97-b36e-b62dfc8dcbae-original.jpeg
[7] https://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf

are demanding that employees who access their personal information should be cybersecurity-certified.

The security problem is amplified in industries with disparate IT systems and the proliferation of paper-based systems and workflows. Out of the gate, organizations across the board are hamstrung by archaic IT systems that aren't interoperable, including IT staff that are being tasked with doing much more with less. BYOD is clearly the accelerant that elevates the risk to sensitive data.



BYOD Fueling the Data Breach Fire

Data breaches are growing in size, according to the Ponemon Institute's study, by 1.8 percent from 2016 to 2017. The study states, "Disruptive technologies, access to cloud-based applications and data as well as the use of mobile devices (including BYOD and mobile apps) increase the complexity of dealing with IT security risks and data breaches." This increased complexity puts yet another strain on already overworked IT security professionals.

Employees with BYOD smartphones and tablets at their fingertips streamline workflows and in theory, create a better work experience, but the gains in efficiency come at a cost. Each device, essentially a computer at arm's length, maintains a connection to the Internet always, either through the phone's carrier network or Wi-Fi. This means any mobile application could have access to your organization's network at any time without the proper security measures enacted on the device – measures such as containerized partitions or VPN security policies.

The problem with mobile applications is that most application developers aren't security professionals. Building feature and function to mobile app developers is paramount to the security of the application. Additionally, hackers are developing games and productivity applications that look like safe mobile applications when in fact, they are malware.

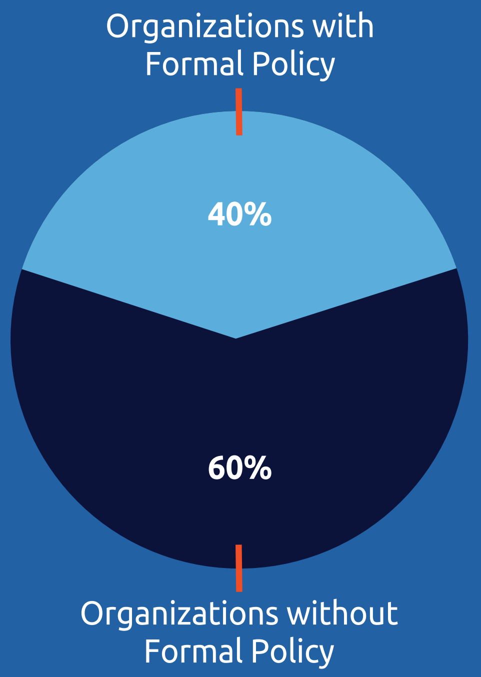
And yet, the bigger problem with mobile applications is that they have access to other applications on the device such as call logs, contact personal identity information (PII), geo-location data, sensitive files and file stores. The mini-computer you have at arm's length if compromised, lost, or stolen, could reveal the keys to your kingdom's data and intellectual property. Because of the robustness of personal data at risk, organizations need to be ultra-sensitive to securing data on these BYOD smartphones and tablets.

5 Things to Reduce BYOD Risk in Your Enterprise

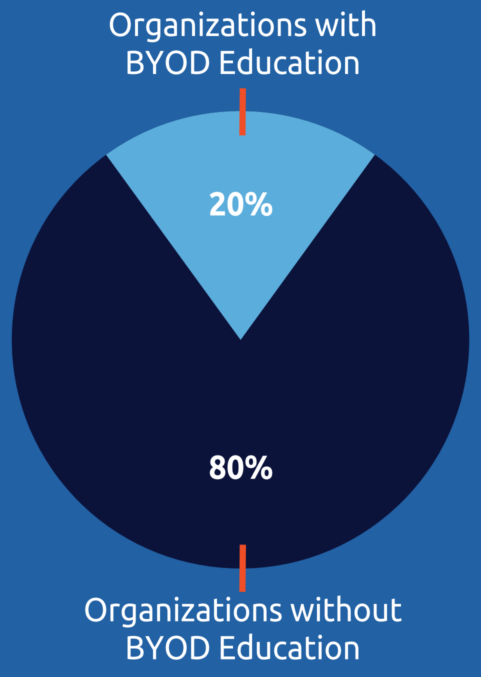
1. Ensure end-point devices are included in your compliance initiatives.

Compliance initiatives for data security such as HIPAA, PCI DSS, GDPR, FISMA and others don't say just secure your servers, desktops and laptops. You must include all event logs from all IT assets, big and small into your SIEM (Security Information & Event Management) systems. Having event logs from endpoint devices alongside servers, desktops and other IT assets in your SIEM provides evidence of security measures in place for all data as well as a visibility across the entirety of the enterprise for anomalous behavior indicative of cyber threat.

Formal BYOD Policy in Organizations



Employee Education Regarding BYOD Risks



From Intermedia, "How BYOD impacts the future of unified communications"

2. Implement containerization with military-grade encryption for data at rest on the device and data in transit to/from your network.

Whether your security administrator(s) are worried about malicious applications on the devices compromising your network, or a lost/stolen device, containerization will provide an extra layer of security at the network endpoint. With a secure and containerized partition on the device, personal applications are segmented from the enterprise applications and data that are being targeted by cyber thieves. Any applications the employee (or contractor) downloads by accident are segmented from your organization's data by the container.

Additionally, if you have NIST-certified (National Institute of Standards and Technology) AES encryption on the container, the data is secured at rest on the device and in transit across your network. SyncDog provides a secure, containerized mobile workspace for productivity applications called Secure.Systems™ (https://secure.systems). Secure.Systems™ delivers FIPS 140-2, AES 256-bit encryption for data on the device and data in transit, and the solution is available from the cloud, on-premise or as a hybrid deployment.

3. Correlate your mobile event log data alongside your other IT asset log data for the true picture of user activity across your network.

BYOD comes with great cost savings to your capital expenditures, but from an InfoSec perspective it is not your friend. A recent article[8] from Intermedia on BYOD cites that 60 percent of organizations operate without a formal BYOD policy in place, and nearly 80 percent of organizations don't educate employees on the risks of BYOD.

[8] https://www.intermedia.net/blog/2017/07/20/how-byod-impacts-the-future-of-unified-communications/

IT Service Delivery is already constrained by the complexity of IT and shortage of IT staff to manage infrastructure and applications within the enterprise network perimeter. BYOD further complicates things for security administrators adding unaccounted endpoint devices at the outer fringes of the network. But if your BYOD policy includes containerization with event log data fed to your SIEM, you can begin to monitor user activity at the far reaches of your perimeter. Including this log data into your SIEM for event correlation – a staple of SIEM systems – can help uncover anomalous behavior across BYOD or within your perimeter that is linked to cyber threat.

4. Have a BYOD policy to stand by and educate your employees on the dangers of BYOD.

As mentioned above, most organizations don't have BYOD policies, nor do they educate employees on the dangers of having a personal device on your organization's network. BYOD education should take place when an employee (or contractor) is onboarded, and then should occur as often as the policy is updated.

As the Society for Human Resource Management (SHRM) points out,[9] much needs to be considered when building a BYOD policy. Enterprise Mobility Management systems are a great starting point because they can control what data employees have access to. But EMM is not security, so you need to fortify your endpoint security with containerization.

Determine what devices your EMM will support and also what level of employee will receive access from their BYOD smartphone or tablet. Also, be sure to let the employee know what rights your organization has to access, monitor and delete information from employee-owned devices. In the E.U., access to employees' phones is restricted and this is another area where containerization is an excellent practice because you can segment PII data from other system data on the device.

5. EMM and Mobile Device Management aren't security systems, and you need to fortify your BYOD policies.

EMM systems were never originally designed as security and anti-virus systems so fundamentally, they cannot operate as efficiently as these systems designed to watch, track then alert on cyber threats as they are happening in real time. Containerization continues to prove to be a highly-effective method of additional security at the device level. A containerized application workspace provides a secure data platform that encrypts and transports data between your enterprise's back-end and a secure, "sandboxed" application container on your employee's mobile devices. This complement to your EMM, provides added security and another layer of difficulty for a hacker to get through to get to your data and corporate IP should the device be lost, stolen or compromised otherwise.

[9] https://www.shrm.org/hr-today/news/hr-magazine/pages/0216-byod-policies.aspx

Conclusion

Hackers are opportunists, and they are constantly looking for the low-hanging fruit to strike and steal data. With so much IT complexity in enterprise environments and lack of IT resources, it's all hands on deck just to keep IT service delivery to acceptable service level agreements. Information Security systems are plentiful, but the chaos of IT complexity and doing more IT work with fewer IT resources rules the day. Within the priorities of InfoSec, smartphones and tablets take a back seat to bigger inside-the-perimeter IT assets like desktops and network servers. And, inside many IT shops, smartphones are viewed as toys, little more than a nuisance that takes IT administrators away from the devices that are more important to running the business.

Much of this InfoSec dysfunction is driven by a disconnect between the business and IT leaders of enterprises. IT as an organizational function is not viewed as strategic and many times is "slave" to the business side of the organization. For BYOD to succeed and for the enterprise's overall InfoSec health, business and IT leaders need to converge and collectively become more strategic.

Aside from the fundamental deficiencies of enterpriseIT, BYOD security must move to the forefront of business strategies. You can fortify your EMM with a containerization solution like Secure.Systems™ and make it more difficult for cyber criminals to breach your perimeter, and they will in turn, gravitate towards easier points of intrusion. Containerization should be a key component of your mobile InfoSec strategy because it makes it harder to hack the device. For more information on the Secure.Systems™ container from SyncDog, please visit https://secure.systems. More information on SyncDog can be found at www.syncdog.com.

SECURE.SYSTEMS
PROTECTED BY SYNCDOG

11950 Democracy Drive, Suite 275
Reston, VA 20190
Call: (703) 430-6040 • Fax: (703) 997-8667
www.syncdog.com • https://secure.systems