2014 SCCE Compliance & Ethics Institute

Tuesday, September 16, 2014 (11:00-12:00 AM)

Session 506

Bring Your Own Device(BYOD)

They are here and they are not going away. Understanding the benefits, risks, and establishing a commonsense strategy for Personally Owned Devices (PODs) in the workplace.

Jim Donaldson

Jim Donaldson, M.S., MPA, CHC, CIPP/US, CISSP

Director of Compliance, Chief Privacy and Information Security Officer
Baptist Health Care Corporation
Pensacola, Florida

Compliance & Ethics Institute
September 14–17, 2014 | Hyatt Regency Chicago | Chicago, IL
BAPTIST HEALTH CARE

Baptist Health Care Corporation

Not-For-Profit Integrated Delivery System
Headquartered in Pensacola, Florida

6671 Employees

Four Hospitals (3 Florida, 1 Alabama)
150+ Employed Providers
Andrews Institute Ortho and Sports Med

Lakeview Center Inc. – Behavioral health
- DUI Program
- FamiliesFirst Network
- Gulf Coast Enterprises (13 States)

Compliance & Ethics Institute
September 14–17, 2014 | Hyatt Regency Chicago | Chicago, IL
BAPTIST HEALTH CARE

Session Goals

- **Understand the various types of Personally Owned Devices (PODs) – You may be surprised.**
- **Understand organizational risks associated with PODs and Bring Your Own Device (BYOD) Programs**
- **Look at strategies for establishing reasonable policies and procedures to mitigate identified organizational risks**

BYOx -

Bring Your Own Anything

What World Changing Event Occurred on June 29, 2007?

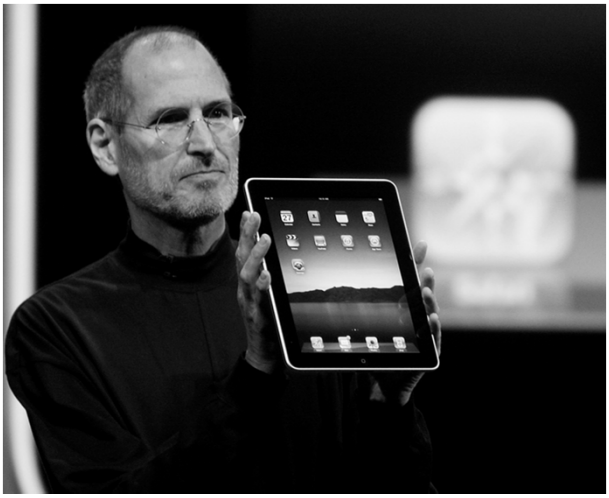
Compliance & Ethics Institute
September 14–17, 2014 | Hyatt Regency Chicago | Chicago, IL
BAPTIST HEALTH CARE

7 years,
2 months
and 14 days ago.

Original iPhone June 29, 2007

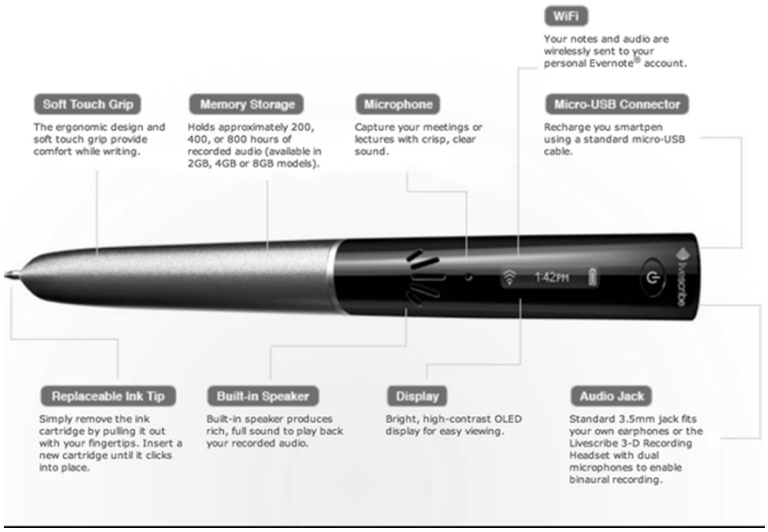
Compliance & Ethics Institute
September 14–17, 2014 | Hyatt Regency Chicago | Chicago, IL
BAPTIST HEALTH CARE

Original iPad April 23, 2010



Examples of BYOx Devices

Smart Pens

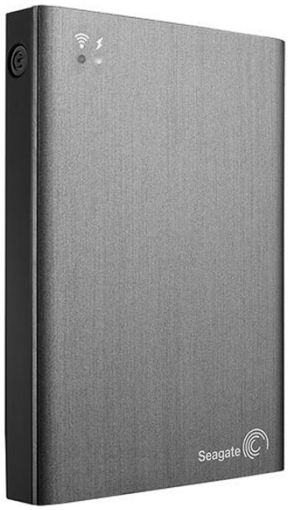


Digital Recorders

Flash Drives

Flash Drives

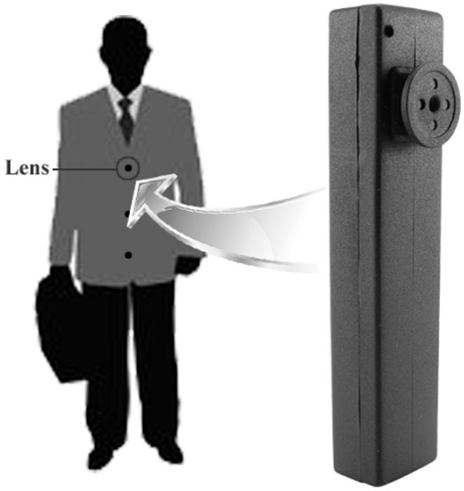
Portable Hard Drives



Navigation Devices

Cameras and Video Recorders

Cameras and Video



Smartphones

Pads/Tablets

Full Size Devices

Mobile Device Characteristics

June 2013 NIST 800-124 R1 Guide for Managing the Security of Mobile Devices

- **Small form factor**
- **Wireless interface WiFi/Cellular/Bluetooth**
- **Built-in data storage (flash memory)**
- **OS that is not a full-fledged OS found on Desktop/Laptop**
- **Applications available through multiple methods Web/App Store/third parties, etc. (jailbreaking/rooting)**

Mobile Device Characteristics

June 2013 NIST 800-124 R1 Guide for Managing the Security of Mobile Devices

- **Camera and/or video capabilities**
- **Audio recording capabilities**
- **Electronic positioning capabilities (NAVSTAR(GPS)/GLONASS/Galileo/BeiDou)**
- **Gyroscopes/accelerometers**
- **Removable Media**
- **Ability to store data for other computing devices**
- **Ability to synchronize with other devices**

Mobile Device Risks

June 2013 NIST 800-124 R1 Guide for Managing the Security of Mobile Devices

- **Lack of physical security – devices are portable by design and vulnerable to theft or loss**
- **Devices may not be trustworthy – For example:**
  - **Has the device been jailbroken or rooted?**
  - **Are there Apps loaded that could contaminate/compromise sensitive data?**

Mobile Device Risks

June 2013 NIST 800-124 R1 Guide for Managing the Security of Mobile Devices

- **Use of untrusted networks – devices are frequently used on multiple networks that may not be configured properly. For example, employee home networks, guest networks at retail outlets, etc.**
- **Interaction with other applications and services – For example:**
  - **Does the device automatically sync with a home computer?**
  - **Does the device automatically sync with cloud based services such as iCloud, Google Drive, Drop Box, Office360, etc.?**

Mobile Device Risks

June 2013 NIST 800-124 R1 Guide for Managing the Security of Mobile Devices

- **Use of untrusted content – Mobile devices may use content that other devices do not normally encounter. For example, the device camera could be used to read QR codes that could link to malicious sites.**
- **Location based services – GPS and network based location services are by default active on most devices. Attackers could use this position data to target the device owner or facilities. For example:**
  - **"Checking in" on Facebook.**
  - **Geotagged data in photos could compromise a sensitive location**

Developing a BYOx Program

- **There is no such thing as one size fits all – tailor your program to your risk appetite. What works in a national security setting may be overkill in other sectors.**
- **Model your strategy around Defense In Depth/Layered security. Consider all mitigating controls that can be put in place to protect your assets and select a combination that mitigates your identified risk.**

Developing a BYOx Program

Gartner defines a BYOD program as:

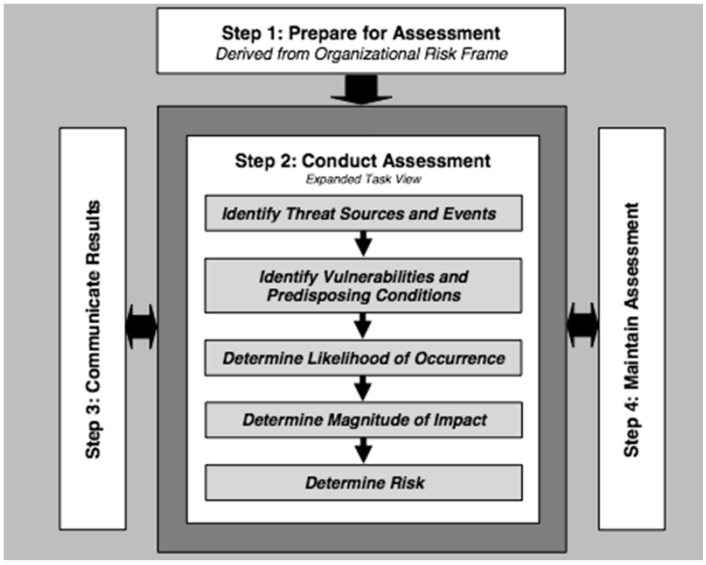
An alternative strategy that allows employees, business partners and other users to use a personally selected and purchased client device to execute applications and access data. It typically spans smartphones and tablets, but the strategy may also be used for PCs. It may or may not include a subsidy.

Bring Your Own Device: The Facts and the Future April 11, 2013

Developing a BYOx Program Risk Assessment

- **Start by conducting a risk assessment to determine how your BYOx program should be developed to address your organizations particular risk.**
- **NIST SP 800-30 Guide For Conducting Risk Assessments**

Risk Assessment Model



Developing a BYOx Program Risk Assessment

- **What will the assessment look at?**
  - **Smartphone/tablets/personal computers**
  - **Personal storage devices**
  - **Personal cameras, recorders, SmartPens**
  - **Cloud based services such as iCloud, Google Drive, Office360**
  - **A combination of the above**

Developing a BYOx Program Risk Assessment

- **What data is your organization trying to protect?**
  - **Proprietary business data**
  - **For official use only government data**
  - **National security data – classified data**
  - **Personally identifiable data**
  - **Medical data**
  - **Financial related such as banking information and credit card data**
  - **A combination of the above**

Developing a BYOx Program Risk Assessment

- **Which laws, rules and regulations are you trying to comply with?**
  - **National privacy laws**
  - **National medical privacy laws (HIPAA/PIPEDA)**
  - **National security mandates**
  - **Financial regulation mandates**
  - **State/Provincial laws**
  - **PCI Standards**
  - **A combination of the above**

Developing a BYOx Program Risk Assessment

- **What are the risks to the information you are trying to protect?**
  - **Unauthorized access**
  - **Manipulation/alteration/Destruction**
  - **Denial of access - the device contains the only copy**
  - **National/state/provincial breach law notifications**
  - **Financial/identity theft**
  - **Medical identity theft**

Developing a BYOx Program

- **Once you have determined the risk factors that need to be addressed by your BYOx program:**
  - **Develop a written policy and procedure that addresses the risks your assessment identified**
  - **Identify/deploy security controls and technology to mitigate risks**
  - **Educate your workforce**
  - **Document that employees understand and agree to comply with the BYOx policy and procedure**
  - **Periodically revaluate and fine tune your program – We are just beginning this journey and BYOx will be a moving target for years**

Device Control vs. Application Containerization

- **Device control through Mobile Device Management (MDM) – Software and communication systems that are used to manage a mobile device.**
- **Application and data containerization through software that encrypts and 'sandboxes' organizational sensitive data from personal data on the device.**
- **A combination of both may be the best strategy**

Technology To Consider

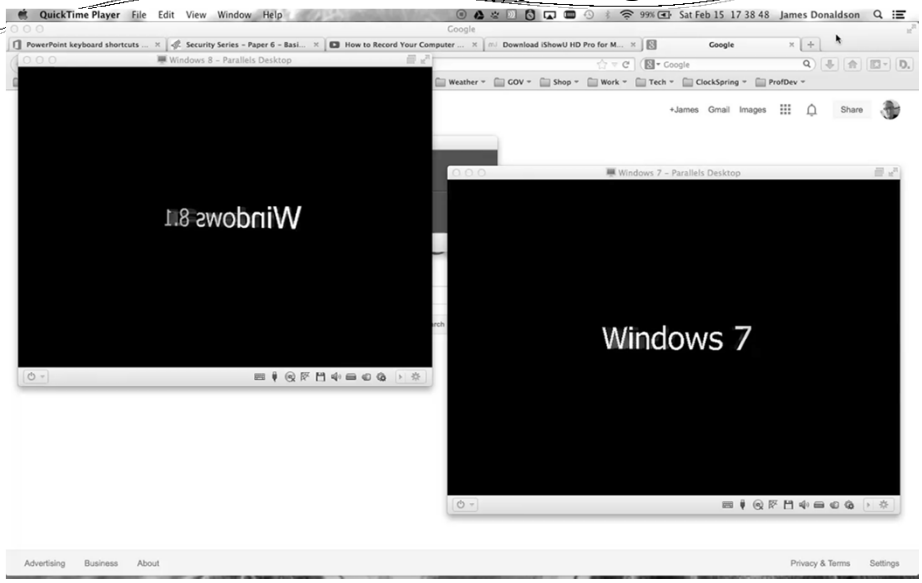
- **Mobile Device Management – Software and communication systems that are used to manage a mobile device.**
  - **Set password requirements (complexity/duration)**
  - **Sets device settings such as time outs**
  - **Whitelists programs**
  - **Device locator services**
  - **Device remote wipe**
  - **Remote device password recovery**
  - **Require certain programs to communicate via organization VPN**
  - **Sets rules on how device services such as the camera can be used**
  - **Force encryption**

  - **<u>Has the potential to irritate your CEO</u>**

Virtualization

- **A virtual computer is a software based computer that is emulated with another computer**
- **A single high-end computer with multiple processors can have dozens of virtual computers operating on the same physical computer**
- **Examples of virtual computing are Citrix and VMware**
- **Excellent way to serve up corporate computing resources securely**
- **Useful when legacy systems won't run on newer operating systems**

Virtual Computing



Remote Desktop Software

- **Technology that allows a user to 'remote' into a computer**
- **Typically a poor user experience on smaller screen devices**
- **Keeps sensitive data on the remote computer**
- **Dependent on active connection between portable device and remote network/computer**

Other BYOx Considerations

- **Which personal devices will you allow your employees to use? SmartPhone, Tablets, SmartPens, etc.**
- **What operating systems will you allow? iOS, Android, BB OS, etc.**
- **How much control will you exert over user devices?**
  - **Remote data wipe**
  - **Remote password resets**
  - **Require/Restrict applications**

Other BYOx Considerations

- **What will you allow employees to do on their device? Email, texting, business apps, Office, remote desktop, virtual computer access, etc.?**
- **How will you handle data on the device if it is lost, stolen, upgraded, rolled down to grandma, etc.**
- **Make sure your BYOx program is tied to your termination process (user management)– make sure the access/data is removed when the person is no longer with the organization**

Other BYOx Considerations

- **Which class of employees will be eligible for the BYOx program?**
- **Are you offering a stipend or other compensation?**
- **Will the program require mandatory participation by certain employees? If the program is new, how do you communicate that to existing employees?**
- **How will the BYOx initiative be integrated into your Information Technology shop from an operational perspective?**

Other BYOx Considerations

- **How will you treat hourly employees? You have to pay them for their time reading emails and texts when they are off the clock.**
- **How will you handle situations that require the organization to take possession of the personal devices? For example, internal investigations, court orders, etc.**
- **How will you handle eDiscovery orders that may involve covered data residing on the personal device?**

Resources

Bring Your Own Device –Toolkit to support agency BYOD programs
http://www.whitehouse.gov/digitalgov/bring-your-own-device
NIST SP 800-30 Guide for Conducting Risk Assessments
http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
NIST SP 800-39 Managing Information Security Risk
http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
NIST SP 800-145 Definition of Cloud Computing
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
NIST SP 800-124 R1 Guidelines for Managing the Security of Mobile Devices
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
***ASD Strategies to Mitigate Targeted Cyber Intrusions – Updated February 18, 2014**
http://www.asd.gov.au/infosec/top-mitigations/top35mitigations-2014-table.htm
***SANS Top 20 Critical Security Controls – Updated to V.5 January 31, 2014**
http://www.sans.org/critical-security-controls/controls
***National Cybersecurity Framework Version 1.0 - Released February 12, 2014**
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Questions?

2014 SCCE Compliance & Ethics Institute

Tuesday, September 16, 2014 (11:00-12:00 AM)

Session 506

Bring Your Own Device(BYOD)

They are here and they are not going away. Understanding the benefits, risks, and establishing a commonsense strategy for Personally Owned Devices (PODs) in the workplace.

Jim Donaldson

Cloud Computing

The <u>Cloud</u> refers to services provided over the Internet

- **Cloud based Software as a Service (SAS) -** EMR, Event Reporting, Survey Tools, LMS, Policy & Procedure management
- **Cloud based transmission and storage -** Google Drive, iCloud, DropBox, Box, Office 360
- **Cloud based email and Calendars -** Gmail, Yahoo Mail, iCloud Mail, Hotmail
- **Cloud based communications -** Skype, Facetime, Voxer
- **Social Media sites -** Facebook, Twitter, Linkedin, Pinterest, Google+