BYOD

LEGAL & TECHNICAL IMPLICATIONS

Online Tech Webinar - November 12 2013

Outline

- Introductions
- Overview of BYOD
- Legal Concerns and Drafting Considerations
- Technical Issues and Considerations
- Questions

t

Tatiana Melnik

- Attorney helping clients protect their data and the data others entrust to them
  - Focus on healthcare IT information technology data privacy and security and intellectual property
- HIT columnist for the *Journal of Health Care Compliance*
- Managing Editor for the *Nanotechnology Law & Business Journal*
- JD BS in Information Systems BBA in International Business

t

Steven Aiello

- Sr Product Architect @ Online Tech
- 15 years experience managing IT in the healthcare and financial sectors
- Bachelors in Technology Management Masters of Science with a focus on information assurance
- Certifications Include
  - CISSP
  - CISA
  - VCP
  - CCNA

s

Outline

- Introductions
- Overview of BYOD
- Legal Issues and Drafting Considerations
- Technical Issues and Considerations
- Questions

s & t

B.Y.O.D Movement – Natural Evolution

- 88% of US adults are cell phone owners (PewInternet, March 2012)
  - 46% of those adults own smart phones
- Forbes:
  The primary business driver is getting work done. Business users do not want to compromise. They want convenience. They want to be able to do the work without being tethered to their laptops. People deserve and demand a great user experience.

s

B.Y.O.D Movement – Single / Dual Use

- Mobile device shift
  - From single use – one for work one for personal
  - To dual use – one device for both work and personal
- Why?
  - Convenience
  - Increased integration of work and personal lives
  - Less maintenance (one phone vs two phones)
  - Cost savings

B.Y.O.D Movement – Cost Savings

- **Case Study**: **Equal Employment Opportunity Commission**
  - In 2011 – EEOC's budget for mobile devices BlackBerry) = $800K
  - In 2012 – Budget reduced to $400K
  - Question?
    - **How do you reduce expenses?**

B.Y.O.D Movement – Cost Savings

- Two-pronged approach to reduce expenses
  - "Negotiate" with wireless carrier
    - Saved $240K
  - Implement a BYOD program

B.Y.O.D Movement – Cost Savings

- BYOD was a good option because there was a **more efficient use of resources**

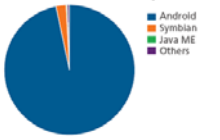
> *"75% of our users never made phone calls from their BlackBerrys ... Email is the killer app. They either used the phone on their desk* ***or they used their personal cell phone to make calls because it's just easier****. We also found there* ***were a number of zero-use devices****. People have them parked in their desk drawer, and the only time they use it is when they travel."* - *Kimberly Hatcher CIO U.S. Equal Employment Opportunity Commission (EEOC) BYOD Pilot*

B.Y.O.D Movement – Employee Satisfaction

- Steven – Multi-vendor / Android
  - Open source open ecosystem
  - No vendor lock in
- Tatiana – Apple / IOS
  - Closed ecosystem
  - Less interoperability concerns
  - Less security concerns

B.Y.O.D Movement – Employee Satisfaction

Total Mobile Malware by Platform



Of 36 699 mobile malware samples 97% of those are for the Android platform.
Source McAfee *Mobile Malware Growth Continuing in 2013* Feb. 2013

Mobile Vulnerabilities by Platform

Platform	Documented Vulnerabilities
Apple IOS	387
Android	13
BlackBerry	13
Nokia	0
LG Electronics	0
Windows Mobile	2

Source Source Symantec Internet Security Threat Report – 2012 Trends vol 18 Pub. April 2013

B.Y.O.D Movement – Strong Support

- **Recognizing the proliferation of mobile technology, HHS has strongly advocated for using mobile devices**
- Improving public health outcomes → drive down healthcare costs
- Helping with chronic disease management
  - Reminding people to take medications
- Reaching rural areas
- Empowering individuals through education

B.Y.O.D Movement – Strong Support

- **Community Partnerships – Text4Baby**
  - Many partners (community and government health orgs wireless carriers businesses)
  - Free text messages to women (i) who are pregnant or (ii) whose babies are < 1 yr old
  - Provides them with reminders and other information aimed at improving their health and the health of their babies

B.Y.O.D Issues – Security challenges

- Personal devices plugged into corporate computer systems via USB
- Personal devices connecting to corporate Wi-Fi networks
  - NAC or MAC filtering for corporate access points
  - VPN access is always wise even for corporate Wi-Fi networks
- Data exfiltration & data theft from lost of stolen devices
  - App ications like office readers on phones
  - Dropbox used to sync documents from a work laptop to a personal phone
  - Potentially sensitive corporate e-mail left on phones

B.Y.O.D Issues – Security challenges

Mobile Threats in 2012

Source Source Symantec Internet Security Threat Report – 2012 Trends vol 18 Pub. April 2013

Outline

- Introductions
- Overview of BYOD
- Legal Concerns and Drafting Considerations
- Technical Issues and Considerations
- Questions

B.Y.O.D Issues – Legal Concerns

- Compliance concerns
  - Healthcare finance insurance highly regulated
  - Compliance with internal controls to protect confidential information
- Breach Notification laws
- Data Destruction laws
- Litigation Holds – Where is your data?
- Wage and Hour laws
- Malpractice issues (doctors attorneys)

B.Y.O.D Issues – Legal Concerns

- Privacy & security issues currently most prominent concerns
  - **Numerous** data breaches resulting from lost/stolen laptops and USB drives
  - Data breaches from devices sold on eBay Craigslist that are not properly wiped

B.Y.O.D Issues – Legal Concerns

- **Industry Example: Healthcare**
  - Legislators raised concerns with using mobile devices for healthcare
    - Safety Security Reliability of the network infrastructure
  - Numerous agencies evaluating issues
    - FDA FCC NIST (Dept. of Commerce) FTC Office of Civil Rights (HHS)
  - State legislators and regulators are also paying attention
    - California is particularly active (http //oag.ca.gov/privacy/privacy-laws)

B.Y.O.D – Corporate Maturity

- Different rules for small companies vs big companies?
  - Office of Civil Rights
  - Fines are designed to send a message
  - In addition there could be class action law suites
  - Litigation is expensive
  - Generally no
  - But penalties may be different
    - Regulatory agencies do generally take ability a company's ab lity to pay nto account
    - Small company pays a f ne of $100K vs. large company pays a f ne of $1.5M per inc dent per year
    - But both pay something....

B.Y.O.D – Policy Drafting Considerations

- **Why have a policy?**
  - To protect your clients / customers / patients' rights
  - To instill professionalism throughout your enterprise
  - To protect your organization from liability
  - To protect your employees from liability

B.Y.O.D – Policy Drafting Considerations

- **Regulators are focusing on mobile devices!**
  - OCR Actions
  - State data breach laws
  - GLBA/FTC Safeguards Rule
  - PCI DSS
  - FDA mobile medical devices/apps
  - California encryption mandates

B.Y.O.D – Policy Drafting Considerations

- **Many Policies *Affect* BYOD**
  - Acceptable Use Policies
  - Security Policies (*e.g.* password encryption)
  - Social Media Policy
  - Remote Access Policy
  - Litigation Hold Policy
  - Remote Working Policy (over 40 hours/wk?)
  - Incident Response Policy
  - Breach Notification Policy
  - Privacy Policies

B.Y.O.D – Policy Drafting Considerations

- **What Kind of Issues Should a Discrete BYOD Policy Address?**
  - http //www.sans org/reading room/whitepapers/pda/security-policy-handheld-devices-corporate-environments 32823
  - Incorporate other related policies by reference (e.g. privacy acceptable use social media etc)

B.Y.O.D – Policy Drafting Considerations

- **Include the right team**
  - Senior management (resources institutional support)
  - Chief IT officer (sets the strategic direction including policy)
  - IT staff (implements strategy/policy)
  - Legal/Regulatory (subject matter expertise/enforcement)
  - Human resources (enforcement)

B.Y.O.D – Policy Drafting Considerations

- **Policies are cited by regulators and plaintiffs' attorneys**
  - When FTC evaluates privacy complaints from consumers it looks to the company's privacy policy
    - Charges brought under Section 5 of the FTC Act - bars unfair and deceptive acts and practices (plus 33 other laws rules and guides providing the FTC with enforcement authority to protect consumers' privacy)
    - "As of May 1 2011 the FTC has brought 32 legal actions against organ zations that have violated consumers' privacy rights or misled them by failing to mainta n security for sensitive consumer information."

B.Y.O.D – Policy Drafting Considerations

- As of May 1 2011 the FTC has brought 32 legal actions against organizations that have violated consumers' privacy rights or misled them by failing to maintain security for sensitive consumer information.
  - 32 doesn't sound like a lot does it?
  - Maybe… but consider – when the FTC takes action most companies enter into a consent agreement where they agree to 20 YEARS of third party audits

"The reporting period for the Assessments shall cover 1) the first one hundred and eighty (180) days after service of the order for the initial Assessment and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments." – *Agreement w th Compete Inc. Cbr Systems Inc. and others*

B.Y.O.D – Policy Implementation

- Review policies and procedures on a regular basis
- Quarterly sign offs and annual reviews
- Lack of diligence on the part of corporate officers

B.Y.O.D – Policy Implementation

- Is your company technically mature enough to enforce the policies its writing?
- What is the security poverty line? https://451research com/t1r-insight-living-below-the-security-poverty-line

B.Y.O.D – Policy Implementation

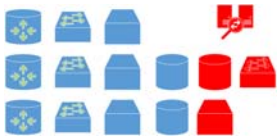
- Mobile device encryption
- Pass code requirements
- Enforce screen lock timers
- Enforce no jail broken phones
- Enforce an enrollment system for remote wipe
- Enforce application and OS update policies

B.Y.O.D – Policy Implementation

- Log review syslog netflow data etc
- Correlation is hard and usually VERY expensive

B.Y.O.D – Data Security

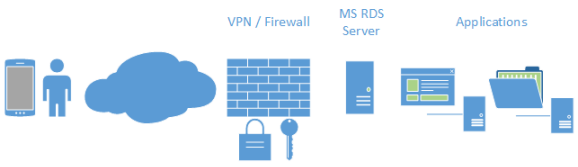
- Data classification: not everything has the same value so separate it
- Data isolation: you can't protect everything so separate it



B.Y.O.D – Data Delivery

- Application Delivery via Microsoft Terminal Server Services
  - Mature technology
  - Well understood easy to support
  - Many clients available
  - Works very well for tablets

B.Y.O.D – Data Delivery

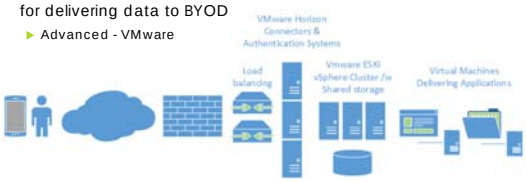


B.Y.O.D – Data Delivery

- Keys to protecting your data
- VPN
  - try and keep services off the open Internet
- 2 Factor Authentication
  - Use it no excuses it's literally free for small businesses
- Strong encryption: Baked in with new operating systems
  - Windows XP end of life April 8 2014 (extended support)

B.Y.O.D – Data Delivery

- Talk about technical solutions for delivering data to BYOD
  - Advanced - VMware



B.Y.O.D – Case Study: Healthcare

- Massachusetts Eye and Ear Infirmary
  - Data breach: Feb 19 2010 – doctor's laptop stolen during a lecture tour in South Korea
    - Impacted data of about 3 500 research participants
  - Report to OCR (HITECH): April 21 2010
  - OCR Investigation Initiated: October 5 2010

B.Y.O.D – Case Study: Healthcare

- Massachusetts Eye and Ear Infirmary
  - Press Release announcing resolution: September 17 2012 → *Almost 2 years*!
  - Financial penalty: **$1.5 million**
  - Corrective Action Plan: **3 years of monitoring**

B.Y.O.D – Case Study: Healthcare

- What did OCR find problematic?
  - MEEI **did not demonstrate** that it **conducted a thorough analysis** of the risk to the confidentiality of ePHI ***on an on-going basis*** [and] did not fully evaluate the likelihood and impact of potential risks to the confidentiality of ePHI maintained in and transmitted using **portable devices**
  - Security measures were not sufficient to ensure the confidentiality of ePHI that it *created, maintained, and transmitted* **using portable devices** to a reasonable and appropriate level

B.Y.O.D – Case Study: Healthcare

- What did OCR find problematic?
  - MEEI did not adequately adopt or implement **policies and procedures to:**
    1. address security incident identification reporting and response
    2. restrict access to authorized users for portable devices
    3. provide it with a reasonable means of knowing whether or what type of portable devices were being used to access its network
    4. receipt and removal of portable devices into out of and within the facility

B.Y.O.D – Case Study: Healthcare

- What did OCR find problematic?
  - MEEI did not adequately adopt or implement **technical policies and procedures to** allow access to ePHI using portable devices only to authorized persons or software programs
  - MEEI had no reasonable means of tracking non-MEEI owned portable media devices containing its ePHI into and out of its facility or the movement of these devices within the facility

B.Y.O.D – Case Study: Healthcare

- What did OCR find problematic?
  - MEEI did not implement an equivalent reasonable and **appropriate alternative measure to encryption** that would have ensured confidentiality of its ePHI *or document the rationale supporting the decision not to encrypt*

Disclaimer

- This presentation is informational only. It does not constitute legal or professional advice.
- You are encouraged to consult with an attorney if you have specific questions relating to any of the topics covered in this presentation.

Contact Details

- Please feel free to contact us with questions:
  - Tatiana Melnik
    - tmelnik@melniklegal.com
    - (734) 358-4201
    - www.melniklegal.com
  - Steven Aiello
    - saiello@onlinetech.com
    - (734) 748-9374
    - www.onlinetech.com/whitepapers

Upcoming Online Tech Events

- Indiana Healthcare Symposium Indianapolis IN
  - November 13 2013
- TechTomorrow 2013 Columbus OH
  - November 14 2013
- Detroit CIO Summit Novi MI
  - November 20 2103
- mHealth Summit Washington DC
  - December 8 – 11 2013