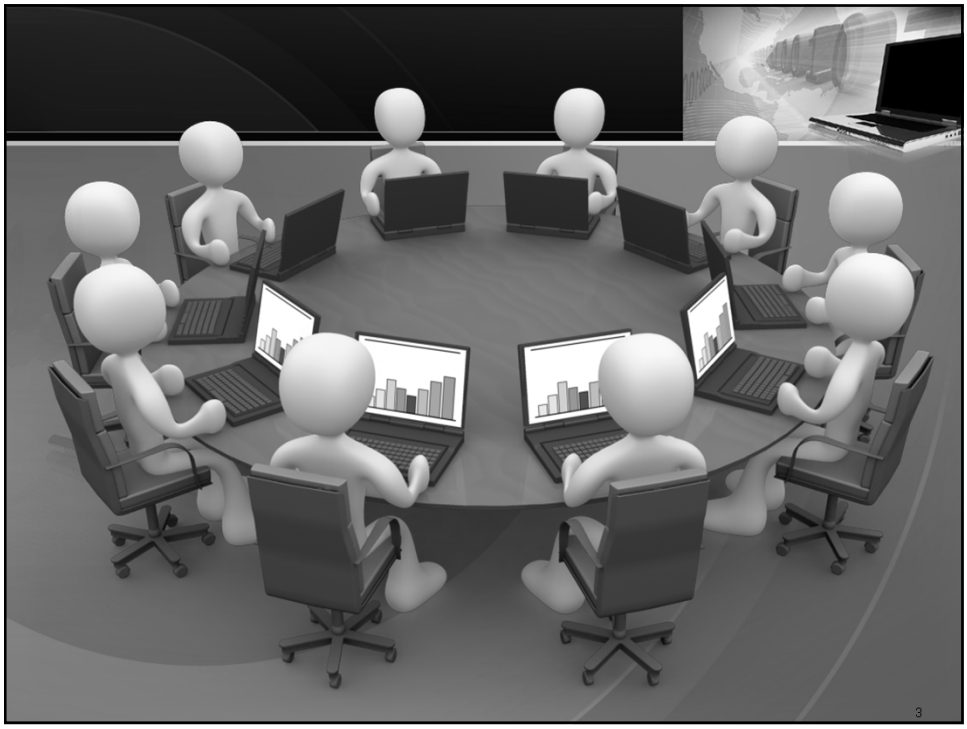
BRING YOUR OWN WHAT?

BYOD
BRING YOUR OWN DEVICE

Agenda

- What is BYOD?
- The BYOD Trend – Evolution of Mobile Technology
- Benefits to allowing BYOD
- Disadvantages of allowing BYOD
- Regulatory requirements and BYOD
- Best Practices for Managing Mobile Device Usage
- Overview of Mobile Device Management Technologies
- BYOD Management Strategies and Trends
- Questions and Answers

2



WHAT IS BYOD?

- Permitting employees to use personal mobile devices to perform work functions
- Devices may include laptops, tablets, smartphones, etc.
- BYOD is a type of Bring Your Own Technology (BYOT)
- Devices typically connect to the corporate network
- Primarily driven by perceived enjoyment

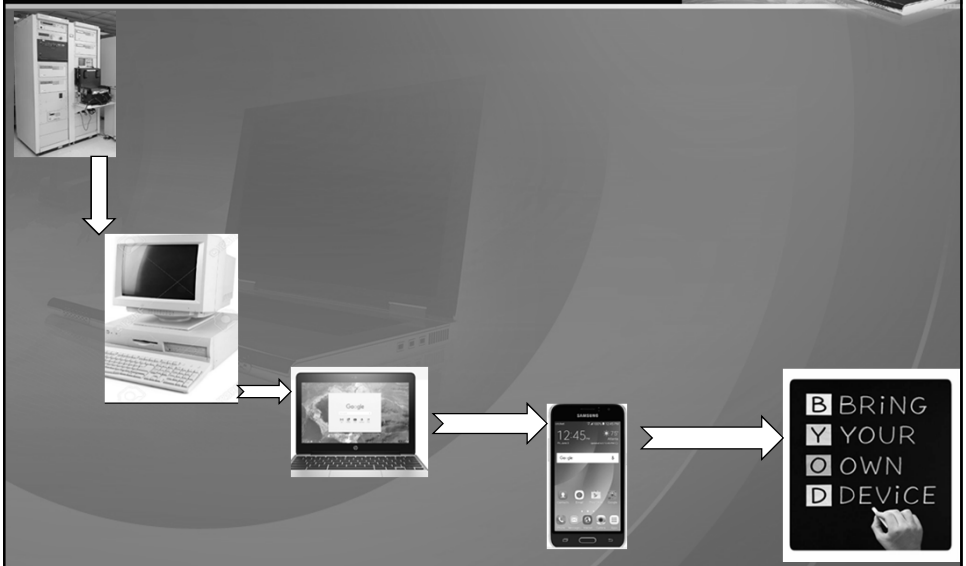
WHAT ARE YOU BRINGING?

- Bring Your Own device (BYOD)
- Bring Your Own technology (BYOT)
- Bring Your Own Phone (BYOP)
- Bring Your Own Personal Computer (BYOPC)

- Fun!!!!!
  - Bring Your Own Demon
  - Bring Your Own Devil
  - Bring Your Own Destroyer
  - Bring Your Own Damage

5

BYOD - A TECHNOLOGICAL TWIST



6

To BYOD or not to BYOD

- It is not a matter of when to allow employees to bring their own devices to work
- It is now a matter of how to manage BYOD in the work place

7

Historical Perspectives of BYOD

- Employee use of company owned computers
  - Using laptops to access the Internet
  - Drove usage policies and technology controls
- Bring Your Own Device' (BYOD) was initiated in the year 2009 by a top IT companies
- By mid-2012, the iPad represents a significant slice of a mobile connectivity pie that will reshape health care
- As of the end of 2013, four out of five medical providers were using their own personal devices at work

8

BYOD Culture

- Consumerization of information technology
- In a 2010 study, 290 million smartphones and 18 million tablets were sold
- In 2014 on Apple's release of its latest iPhone, 4 million were sold on the first day
- 2015 reports state that the number of mobile devices worldwide has grown to over 2 billion

9

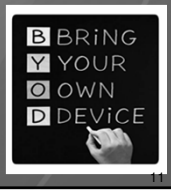
Care Thread Survey on BYOD

- A survey by Care Thread found
  - Clinicians use 6.4 different mobile devices in a day on average according to IDC Healthcare Insights Study
  - 69% of the consumers surveyed said they were concerned about the privacy of their medical information if providers accessed it through their mobile devices
- Beware of legal ramifications

10

Aruba Survey on BYOD

- In a survey from Aruba Networks, 85% of respondents said their organization has a BYOD policy, but implementation was inadequate
- 53% of respondents said their organization only allows personal mobile devices to access the Internet
- 24% said their organization provides personal mobile devices with limited access to hospital applications
- 8% said their organization provides personal mobile devices with full access to the hospital network



11

Benefits of BYOD

- Benefits
  - Improved responsiveness
  - Improved accessibility
  - Greater flexibility
  - Reduced equipment costs

12

More Benefits of BYOD

- Increased productivity provides access to:
  - Advanced technology
  - Personal applications anytime
- Workforce Mobility leads to:
  - An increase in employee satisfaction
  - A role change – now called “mobile workers”
- Cost Savings:
  - Hardware – employees purchase their own
  - Decrease in support

13

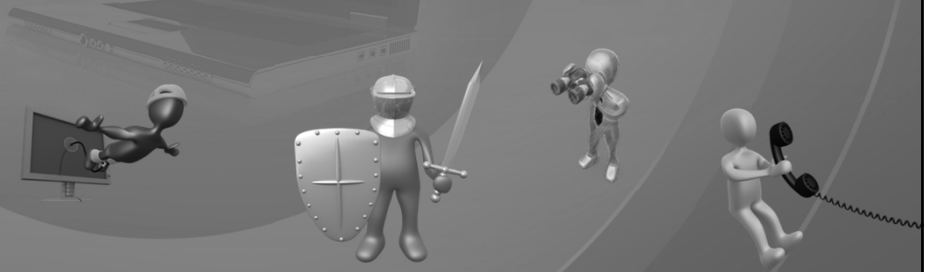
Challenges of BYOD

- Challenges
  - IT support of a wide range of mobile vendors and operating environments
  - Secure access to enterprise data
  - Mitigate risk of unsecure personal apps
  - Ensuring minimum security baselines
  - Data commingling
  - Liability issues

14

DISADVANTAGES OF BYOD

- *A 2012 Global State of Infosecurity Survey found*
- 70 million Smartphones were lost or stolen in 2011
- Of these, only 7% of devices were recovered
- 17% of businesses have mobile device breaches



15

MORE DISADVANTAGES OF BYOD

- Malicious threats
- Control application portfolio
- Lost and stolen phones
- Access control and auditing
- Compliance
- Growing device inventory
- Native functions and features are inadequate
- Changes to Microsoft Exchange licensing costs

16

BYOD Risks

Risk Issues	Types of Risks
Security	• Misuse of mobile technologies • Lost or stolen personal devices
Human Resources	• Labor laws – employees working after hours • Subsidies/reimbursement cost – taxable income?
Legal Implications	• Confidentiality of corporate information • Storing sensitive information on personal devices
Hidden Costs	• IT/Network infrastructures • Support Systems – multiple device users • Application usages • Compliance management

17

REGULATORY REQUIREMENTS AND BYOD

- HIPAA
- HITECH
- CMS
- PCI/DSS
- SOX

18

HIPAA AND BYOD

- According to a 2014 research report:
  - 17 million health applications available in major app stores
  - Designed primarily for healthcare professionals
  - Types of apps focus on CMEs, remote monitoring and health care management.
- Case Study:
  - Miami Children's Hospital
  - Outcomes of their strategic business goal:
    - Enriched patient experiences
    - Improved patient care
    - Increased brand awareness

19

HIPAA, HITECH, PHI, and BYOD

To protect personal health information (PHI) and to avoid the pitfalls of BYOD

Always use HIPAA and HITECH guidelines for sending PHI

20

Positive Aspects of BYOD in Healthcare Facilities

- Requires less or no training on the device
- More reachable clinical staff at any hour
- Less costly than purchasing separate mobile devices for staff and employees
- More convenient to have one device for both personal and professional uses
- The belief that having a personal device at work enhances morale and improves productivity

21

Best Practices of BYOD in Healthcare Facilities

- A decisive mobile device policy
- Healthcare IT control and management
- Security procedures in place
- Liability coverage due to HIPAA non-compliance
- Employee training and awareness

22

BYOD Dos in HIPAA

1. Make sure your vendor and its sub-vendors are complaint with the new HIPAA Omnibus requirements
2. Use two levels of security upon login to enterprise apps
3. Have the capability to remotely wipe a device if it is missing

23

BYOD Don’ts in HIPAA

1. Do not allow PHI or any info to be written to the mobile device
2. Do not permit integrations with insecure file-sharing or hosting services

3 Do not set the BYOD and forget it

24

BYOD Don'ts in HIPAA

1. Do not allow PHI or any information to be written to the mobile device
2. Do not permit integration with insecure file-sharing or hosting services
3. Do not set the BYOD and forget it

25

CMS AND BYOD

- Aruba Networks, Inc. recently released the results from a survey focused on the networking priorities of more than 130 healthcare
- Seventy-six percent of respondents said that they provide Internet access to patients and visitors, with 58 percent doing so through open networks with no password protection.
-
- Seventy-five percent also noted that their hospital applications were available remotely to clinics, physicians and others.
- 85 percent of respondents said that they are supporting their physicians' and staffs' use of personal devices at work.

26

PCI/DSS AND BYOD

- PCI has eight sub-requirements that require:
  - Explicit approval by authorized parties
  - Authentication for use of the technology
  - A list of all such devices and personnel with access
  - Labeling of devices to determine owner, contact information and purpose.
  - Acceptable uses of the technology
  - Acceptable network locations for the technologies
  - List of company-approved products
  - Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity

27

PCI/DSS AND BYOD

- Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet
- Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs).
- Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.
- Incorporate two-factor authentication for remote access

28

PCI/DSS AND BYOD

- Require a minimum password length of at least seven characters
- Use passwords containing both numeric and alphabetic characters
- Limit repeated access attempts by locking out the user ID after not more than six attempts. Some security systems may not be able to enforce this without wiping the device
- Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID
- If a session has been idle for more than 15 minutes; require the user to re-authenticate to re-activate the terminal or session
- Implement automated audit trails for all system components to reconstruct events.

29

SOX AND BYOD

- SOX aims at tightening corporate accountability, in part by requiring businesses to establish, maintain, and report adequate internal controls
- Sarbanes Oxley (SOX) set security standards and policies to protect confidential corporate and financial data
- For SOX and BYOD to coexist, a solution to secure corporate data and keep it off personal devices is necessary. Use VMware
- The concept of the “data less tablet” or smartphone that can meet SOX security requirements is now possible

30

Legal AND BYOD

- Courts are now catching up to BYOD with rulings to be considered in shaping BYOD policies.
- Partitioning Work-Related Content from Personal Content?
- Employers should review their BYOD policies and make sure that employees know the circumstances under which a device may be wiped
- Which Employees Should Be Part of a BYOD Policy?
  - Exempt Employees
  - Nonexempt employees
  - Contractors
  - Others

31

More Legal AND BYOD

- Reimbursing Your Employees for Their Devices?
  - If you partially reimburse employees for using their personal devices for work purposes, is there any legal ramification is that employee' device is hacked and the process affect company data?
- BYOD vs Litigation Hold?
  - BYOD complicates the e-discovery process because electronic data that may fall within the scope of discovery requests can reside on devices besides those over which the company has control.

32

CYBER CRIME AND BYOD

- Bring Your Own Device (BYOD) to work policies for mobile devices could introduce more risk of cybercrime to employers
- In a recent study, Norton found that 431 million adults or ten percent of adults have experienced cybercrime on their smartphones at an annual cost of $114 billion
- Cybercrime refers to crime using the internet, such as stealing bank or corporate intellectual property. Employees' mobile devices may be more susceptible than ever because employers have limited controls for employees that use their personal devices at work

33

CYBER CRIME AND BYOD

- While 74 percent of respondents in the Norton survey indicate that they are aware of cybercrime threats
- Only 41 percent of adults have up-to-date software to protect them from this problem
- Less than half or 47 percent review credit card statements regularly for fraudulent activity
- 61 percent do not use complex passwords
- Hackers seek to exploit unprotected employees' devices as entry points to mine sensitive data on the network

34

ESPIONAGE, Insider Threat, and BYOD

- It is increasingly accepted that insiders represent the greatest risk to organizations' security particularly when considered as an element of a converged threat to intellectual or digital assets.
- The challenging aspects of the insider threat are the anticipation of both intent and method.
- Industry is increasingly aware of disgruntled employees as a source of threat

35

Best Practices

- Registering devices to ensure security:
  - Virus protection, authentication, encryption
- Provisioning of firm-authorized apps
- IT use monitoring
- User education
  - Compliance with firm security policies
  - Mobile Device registration with IT
  - Password protection
  - Use of unsanctioned apps
  - Lost/stolen devices

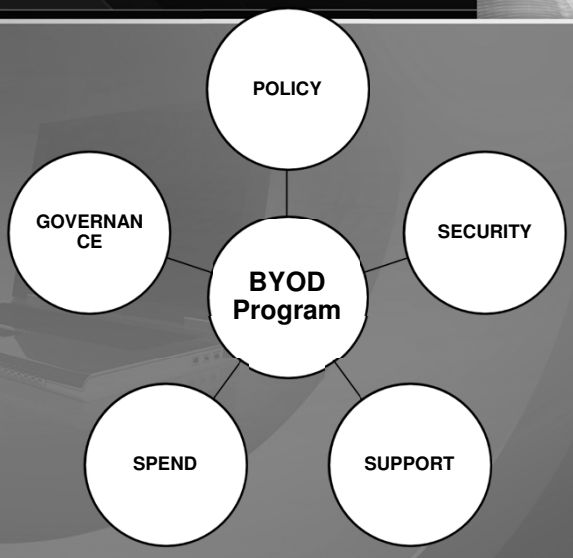
36

COMMON ATTACKS ON BYOD

- Email
- Download scripts to attack
- Buy software to attack
- Hire a company to help in the attack

37

What is a BYOD Program?



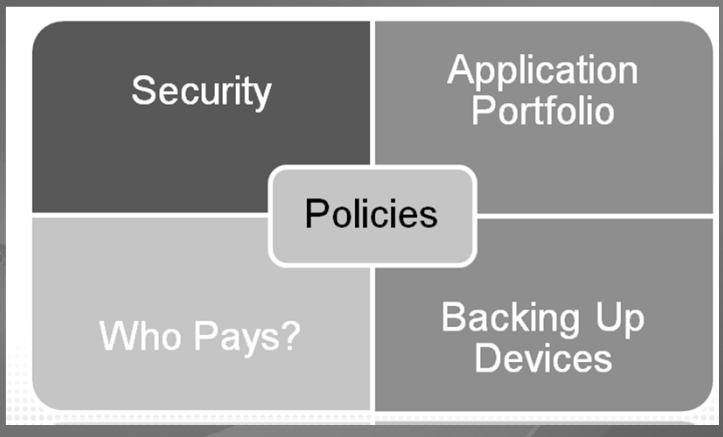
38

BYOD Program Best Practices

- Data protection and security
- Employee privacy
- Policies to deal with theft or loss
- Non-exempt employee usage
- Workforce training and engagement

39

BYOD – MOBILE DEVICE MANAGEMENT



40

MDM SOFTWARE

- Who is responsible for equipment?
- IT staff availability and training
- Mobile device OS and security upgrades
- Mobile Device Management platform
- Is your firm website mobile friendly?

41

Mobile Device Management

- Not new!
- Optimize functionality
- Increase security
- Compliance
- Is MDM a requirement for BYOD?

42

MDM Selection Criteria

- Enrollment
  - Ease
  - Self service
- Administration
- Ongoing Management
- Scalability
- Device Support

43

MDM MAGIC QUADRANT

44

Common Features

- Device provisioning and configuration
- Policy application
- Security
- Backup / restore
- Remote lock and wipe
  - Sandboxing
- Activity logging
- Reporting / dashboard

45

Advanced Features

- Network access control
- Application deployment and management
- Firmware updates
- Diagnostics
- Network usage and support
- Mobile asset tracking and management
- Troubleshooting and diagnostic tools
- Remote control
- Remote administration
- GPS tracking and 'breadcrumb' mapping

46

Most Common MDM Platforms

- Airwatch
- MobileIron
- McAfee
- Fiberlink (MaaS360)
- Cisco Meraki MDM

47

Future of MDM

- Commoditized
- Management tools with features built into devices
  - Open Mobile Alliance (OMA)
  - OMA Device Management Protocol
- MDM absorbed into management platforms
  - Mobile Application Management (MAM)
  - Mobile Information Management (MIM)

48

BYOD Policy

- Mobile health devices and BYOD policies provide healthcare professionals with the ability to facilitate smoother workflows, promote team collaboration and help boost productivity.
- Develop Policy awareness & Assess the understanding of the policy
- Develop Questions and Answers of the Policy
- Work with the Policy Committee and the users
- Re-evaluate the policy
-

49

THANK YOU

50

CONTACT

Milton Kabia, Ph.D., CISPP, HCISPP, SCNA, ITIL

Sr. Information Systems Security Officer

Alaska Native Tribal Health Consortium (ANTHC)

Office – 907-729-2699

Cell – 907-351-5825

E-mail: mkabia@anthc.org

51