fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

BYOD (Bring Your Own Device) Panel

FISSEA - 26th Annual Conference

Gaithersburg, Maryland

Thursday, March 21, 2013

Kim Hancher
Chief Information Officer
Equal Employment Opportunity Commission

Tijan Drammeh
Information Systems Security Officer
Organization: Washington Metropolitan Area Transportation Authority

Andrew Gaither
Senior Information Security Analyst
University of Maryland University College

Moderator – **Dr. Loyce Best Pailen** UMUC

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

Kim Hancher
Chief Information Officer
Equal Employment Opportunity Commission

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

One Agency's Story:
To BYOD or NOT to BYOD

http://www.fedtechmagazine.com/article/2012/10/byod-or-not-byod

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

Federal BYOD Guidance & Toolkit

- Case studies
- Sample policies

http://www.whitehouse.gov/digitalgov/bring-your-own-device

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

BYOD Collaboration Website

A Community of Practice

http://www.advancedmobility.ning.com

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

Tijan Drammeh
Information Systems Security Officer
Washington Metropolitan Area
Transportation Authority

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

BYOD

The rules have changed

- Employees want to use a device of their choice
- Employees are willing to pay for the devices
- How much control can the organization assert
- Support for multiple Operating Systems is needed
- Increased productivity and retention
- Presents new challenges for IT security

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

Implementing BYOD

BYOD Policy

- Policy must be in place and well thought out
- Policy must be approved at the highest level of the organization
- Policy must address the following areas
    - Compliance and audit reports
    - Authentication mechanisms
    - Remote device management
    - Data management
    - Access revocation
    - Application control
    - support provided

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

Implementing BYOD cont'd.

Infrastructure

- **Separate wireless networks**
  - Guest wireless network for non-employees
  - Trusted wireless network for employer issued devices
- **Access Control**
  - user based through AD or LDAP
  - device based using certificates
  - A combination of the above
- **Device Management**
  - remote wipe of devices
  - security policy on devices

BYOD Infrastructure

- Mobile Device Management (MDM)

  - manage corporate or personal devices
  - device provisioning
  - remote configuration
  - certificate management
  - email and application management
  - security management

BYOD Infrastructure cont'd.

- Network Access Control (NAC)
  - automate device enrollment and registration
  - identify unmanaged devices and apply policy
  - block unknown or prohibited devices

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

Conclusions

- Opportunity for organizations, but an appropriate strategy must be developed
- Security and financial exposure must be considered before implementing a BYOD policy
- Employee awareness training must accompany BYOD
- Appropriate technology must be deployed to manage devices and control access to organizational information assets

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

Andrew Gaither
Senior Information Security Analyst
University of Maryland University College

Traditional Security Measures

- Determine and limit the type of devices that can be used
- Implement minimum system requirements and configurations
- Install security-related software to the device
- Encrypt company data on the device
- Apply security patches
- Monitor the use of the device to detect misuse, hacking or malware
- Dictate how the device connects to the company's network
- Install and update anti-virus software
- Provide support for the device
- Obtain/access the device for purposes of an investigation (because the company owns the device).

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

Security Challenges

- **Lack of control over device, data and security**
  - Jailbroken/modded/rooted devices
  - Mobile nature / lost devices
  - More opportunities to pick up virus/get hacked
  - End User lack of IT / security knowledge sophistication (e.g. configurations, patching, anti-virus)
- **Multiple device-types and operating systems**
  - May need to be treated/configured/secured differently
  - May pose different levels of security risk
  - Constant change – No standardization new devices getting popular all the time
- **Think beyond the device**
  - Offsite data transfer ("the Cloud"; auto back-up)
  - Applications
  - Social media access and social engineering/social media hacking
  - Device as portal to entire company network

Security Challenges
Consistency and Legal Risk

- **Reasonable security factors**
  - Sensitivity of the personal information,
  - Likelihood of damage
  - Medium and format of the record
  - Potential harm from an incident
  - Cost of preventive measures

- **Specific security controls required by law or contract**
  - Mass personal information protection law

- **Comply with own policies**
  - Acceptable risk
  - Subjective reasonableness

fissea
Federal Information Systems Security Educators' Association
AWARENESS • TRAINING • EDUCATION

Additional Questions?

If you have additional questions, please send them to
Dr. Loyce Pailen

loyce.pailen@umuc.edu