Avoiding a BYOD Headache

Key Legal, Technical, and Administrative Statements for your Information Security Policies

Presented by **Kelli Tarala**

Principal Consultant Enclave Security

AuditScripts

2

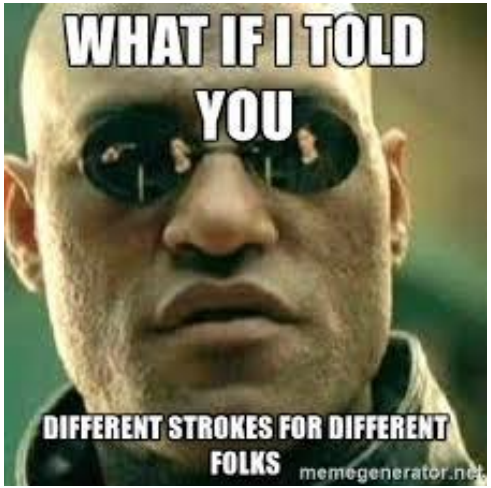
Examine Organizational Strategy

- Do you have a strategy today?
- Don’t ask, don’t tell
- Corporately owned, personally enabled (COPE)
- Choose your own device (CYOD)
- Bring your own device (BYOD)
- Nuclear Option

AuditScripts

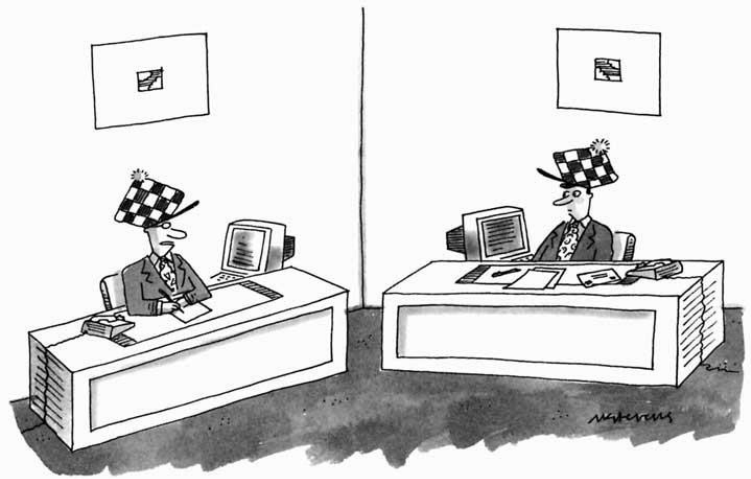
Why are we talking about this?

- Avoid data loss
- Poor performing corporate devices
- Avoiding constraints, technology restrictions
- ‘Unacceptable’ customer service from Help Desk



Organizational Strategy

- Determine which regulations and standards apply to your organization
- Create a strategy based on organizational culture
- Involve multiple departments
  - HR, Legal, Risk Management, Compliance, IT
- Get employee feedback



"I don't know how it started, either. All I know is that it's part of our corporate culture."

Solution: Policy and Technical Statements

- Policy statements that address
  - Administrative, Legal, Human Resources and Employment Issues
  - Cultural: The use of a personally owned device is privilege and may be revoked.

- Technical Statements and Procedures
  - Configurations Standards
  - Outdated Devices
  - Network Monitoring
  - Hardware and software controls
  - Data controls

Policy Statements: Monitoring and Logging

- Preserve the company's right to inspect and monitor
- Banner Statements
- No Trespassing

Policy Statements: Monitoring and Logging (1)

- United States: wide latitude for employers to monitor corporate owned assets
- Banners define a perimeter, and allow for employee consent
- Establish Acceptable Use

Legal
Appropriate
Responsible
Kind

Policy Statements: Monitoring and Logging (2)

- Employee monitoring: Third Party Services
- Potential liability for accessing password-protected services or personal communications under anti-hacking and wiretapping statutes
- Case law protecting attorney-client communications

Policy Statements: Acceptable Use

- Start with what is not acceptable
- Using corporate computing resources for illegal activities is strictly prohibited
- Harassment, Mail bombing
- Placing another workforce member's name on a mailing list

Policy Statements: Internet Acceptable Use

- All internet access and activities will be logged in accordance with the Logging and Monitoring Policy
- All data that is composed, transmitted, and received by this organization's computing resources is considered to belong to this organization and is recognized as official, business data.
- It is subject to disclosure for legal reasons
- This organization may choose to deny communications with (or limit data flow to) known malicious IP addresses (black lists) or limit access only to trusted sites (white lists) in accordance with the Network Security Policy.

Policy Statements: Email Acceptable Use

- Decide limits on personal use of corporate email
  - When, where
  - workforce member's personal agenda such as promoting upcoming parties or political/religious beliefs
- Workforce members should retain only those email messages needed to conduct business on a day-to-day basis or provide documentation for archival purposes.
- Emails pertaining legal matters will be kept according to the litigation hold directions received from Legal.

Policy Statements: Social Media Acceptable Use

- Workforce members must get authorization before commenting about this organization's services or products on social networking sites as a representative of this organization
- If authorization is given, the workforce member must disclose his or her employment relationship with this organization when posting a comment regarding its services or products
- Have a disclaimer that specifically states the opinions and attitudes expressed are those of the workforce member alone and may not be attributed to this organization.

Policy Statements: Social Media Acceptable Use

- Prohibit the unauthorized use of trademarks
- Seek permission of from owners of copyright-protected works such as music, videos, photos
- Prohibit disclosure of sensitive, proprietary, financial, or confidential information
- Establish procedures for the use of the organization's logos and trademarks

Policy Statements: Acceptable Use

- Prohibit unlawful uses
- Describe limits on personal use
- Address off-hours use by non-exempt personnel
- Email sent via corporate system becomes corporate asset
- Write policies acknowledging insider threat
- Awareness training
- Click to Connect or a Network Driver's License

Policy Statements: Data Classification

- Establish clear ownership of the data
- Establish a data custodian
- Establish a simple three-tiered system
  - Public, Private Business Use Only, Highly Confidential
- Tiers should be linked to defined risk levels
- Establish where data can and cannot be stored
- Draw clear lines that sensitive data and client data cannot be stored on device or device must be encrypted

Policy Statements: Data Classification

- Establish where data can and cannot be stored
- Draw clear lines that sensitive data and client data cannot be stored on device or device must be encrypted
- Data retention
- Data destruction

Policy Statements: Data Classification

- It's not the device, it's the data
- As a data controller, the employer must ensure that "appropriate technical and organizational measures shall be taken against accidental loss or destruction of, or damage to, personal data."

Policy Statements: Summary

- Monitoring and Logging
- Acceptable Use
  - Email
  - Internet
  - Social Media
- Data Classification

Technical Statements: Overview

- Use technology to support your policy
- First you say it, then you do it.
- Focus on:
  - Device Security
  - Network Monitoring and Logging
  - Data Classification and Data Controls

Technical Statements: Devices

- The organization will maintain an inventory that contains at a minimum
  - The system's hardware configuration;
  - All approved software installations;
  - All authorized system user accounts.
- Each mobile device will be centrally managed via the organization's system management and configuration utilities

Technical Statements: Devices

- Data shall not be stored unnecessarily on this organization's mobile devices.
- The organization shall not be responsible for backing up data on each mobile device.
- The organization shall utilize host-based data loss prevention tools to help ensure that data is only stored on appropriate devices.
- All mobile devices shall be configured to utilize whole-disk encryption

Technical Statements: Devices

- Devices will be centrally managed and subjected to:
  - Standard configurations
  - Minimum security baseline requirements based on Data Classification system
  - Regularly applied security updates
  - Regularly applied application updates
  - Routine vulnerability scanning and monitoring
  - Unauthorized applications will be removed

Technical Statements: Networks

- All inbound and outbound traffic on boundary network devices will be verbosely logged, including both traffic that is allowed and disallowed
- This organization shall install and maintain intrusion detection and intrusion prevention sensors to record at a minimum all packet header information of traffic destined for corporate networks or passing through a boundary device

Technical Statements: Know Thy Network (1)

- Document standards for monitoring and logging events:
  - Identification mechanisms such as user IDs;
  - Dates and times of key events;
  - Successful and rejected attempts to access data or computing resources;
  - Successful and rejected attempts to evaluate access to a privileged state;
  - Account management activities including password changes;

Technical Statements: Know Thy Network (2)

- Standards document for monitoring and logging events:
  - Source and destination IP addresses;
  - Packet headers information at a minimum, if storage space allows, full packet headers, and full traffic playload;
  - All logs, generated from routine vulnerability scanning procedures
  - Account management activities including password changes

Technical Statements: Data Classification

- Data Classification levels
- This organization will deploy an enterprise-wide data loss prevention tool or another similar tool that monitors for sensitive information leaving corporate networks and alerts system personnel for attempts to ex-filtrate data

Technical Statements: Summary

- Standard Configurations
- Minimum security baselines
- Vulnerability Scanning
- Comply to Connect

In Summary

- Policy statements address company's culture and expectations
- Technical statements tell how it is going to be done
- Back up your BYOD strategy with robust practical processes
- Evaluate corporate IT practices
  - Customer Service, mobile devices
- Awareness Training
- Introduce easier ways for colleagues to share information securely.

Resources

- There are a number of good websites to consider, too many to list on one slide
- A few critical, independent sites to consider are:
  - Center for Internet Security (CIS) Critical Security Controls
  - NIST Special Publications (SP)
    - 800-124 Guidelines for managing the security of mobile devices in the enterprise
  - The SANS Institute
  - AuditScripts.com Free Resources
  - NIST National Checklist Program (NCP)
  - NSA Security Guides

Further Questions

- Kelli Tarala
  - E-mail: kelli.tarala@enclavesecurity.com
  - Twitter: @KelliTarala
  - Website: http://www.auditscripts.com/

AuditScripts