BYOD: Bring Your Own Device

Security & Risk Concerns
What’s This “BYOD” Thingy?

BYOD: BRING YOUR OWN DEVICE
BYOD & BYOMD Defined

• In the Broadest Sense
  • A specialized program designed to provide device independence to end users

• Common Implementation
  • End users provide their own mobile phones
  • End users use personal tablet devices at work
  • Employer subsidized personal computer devices for business use
  • Unsubsidized devices required for business use
Why BYOD?

- Real or Perceived Cost Savings
- Employee Morale and Retention
- Elimination of Certain IT Functions
- Greater Mobility and Flexibility
- Transfer of Risk
Top Security & Risk Concerns

BYOD: BRING YOUR OWN DEVICE
Define Risk

Risk = Asset \times Vulnerability \times Threat

- Asset
  - Resource that has value to the organization

- Vulnerability
  - Weakness of an asset which can be exploited

- Threat
  - Someone or something which will act on a vulnerability
Asset Elimination

• No device ownership = no asset

• Fill in the risk equation

• Anything multiplied by “0” equals “0”
Data: The “New” Asset

• Data becomes the “new” asset

• This is actually a good thing

• Puts security and risk in the proper perspective
Securing Data

• Can sensitive data be stored unencrypted on a device?

• Is any sort of desktop or application virtualization used?

• Could undetected proxies be used at public Wi-Fi sites?
Ways to Defeat Virtualization

- Keystroke logging
- Screen capture or scraping
- RAM dumps
Device Vulnerabilities

• They still exist

• Organizations now have less control over devices, and thus the vulnerabilities

• May be unable to report on vulnerability status
  • Anti-Virus
  • Patches
  • Firewall
Compliance Concerns

Payment Card Industry – Data Security Standard

- Personal firewalls must be installed
- It must be configured by the COMPANY!
- How will you helpdesk support every firewall software on the market?

1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization’s network.

1.4.a Verify that mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), and which are used to access the organization’s network, have personal firewall software installed and active.

1.4.b Verify that the personal firewall software is configured by the organization to specific standards and is not alterable by users of mobile and/or employee-owned computers.
### Compliance Concerns

#### Payment Card Industry – Data Security Standard

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).</td>
<td>5.1 For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.</td>
</tr>
<tr>
<td>5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.</td>
<td>5.1.1 For a sample of system components, verify that all anti-virus programs detect, remove, and protect against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits).</td>
</tr>
<tr>
<td>5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.</td>
<td>5.2 Verify that all anti-virus software is current, actively running, and generating logs by performing the following:</td>
</tr>
<tr>
<td>5.2.a Obtain and examine the policy and verify that it requires updating of anti-virus software and definitions.</td>
<td></td>
</tr>
<tr>
<td>5.2.b Verify that the master installation of the software is enabled for automatic updates and periodic scans.</td>
<td></td>
</tr>
<tr>
<td>5.2.c For a sample of system components including all operating system types commonly affected by malicious software, verify that automatic updates and periodic scans are enabled.</td>
<td></td>
</tr>
<tr>
<td>5.2.d For a sample of system components, verify that anti-virus software log generation is enabled and that such logs are retained in accordance with PCI DSS Requirement 10.7.</td>
<td></td>
</tr>
</tbody>
</table>
Privacy Concerns

Electronic Communications Privacy Act (ECPA)

• Monitoring of Communications

• Voice, Video, IM, Email, etc.

• Business vs. Personal Use
Search & Seizure

• State and federal laws may prohibit employer search or seizure of personal devices

• Policies are worthless if they violate laws
Remote Wipe

• What are you legally allowed to wipe?

• What liability is incurred by the company if you wipe data that wasn’t authorized?

• Remote wipe is worthless unless the data is encrypted to begin with.
Legally Defensible Security

• Risk and security decisions are typically made after due diligence is completed

• Provides some protections for the employer which may be lost if employees don’t do the same thing.

Take Away Points

• Are you prepared to implement the infrastructure required to secure the data on devices you cannot control?

• Can you maintain compliance with regulations or industry standards if employee owned devices are utilized?

• Is your staff prepared to support these systems?
Take Away Points

• Are you able to effectively monitor devices for compliance to the BYOD policy or guidelines?

• Can you ensure a defensible legal position for all security and risk management issues that may arise?

• BYOD programs must include IT, Security, HR, Legal and Privacy professionals to address all of the concerns.
Question and Answer
Thank You

Dave Nelson, CISSP
515-965-3756
dave.nelson@IntegritySRC.com
www.IntegritySRC.com/blog
LinkedIn DaveNelsonCISSP
Twitter @IntegrityCEO