Best Practices for a BYOD (Bring Your Own Device) World

Sangameswaran (Sangam) Manikkayam Iyer – GSEC, CISSP, CISM, CRISC, CCSK

Senior Security Specialist
Symantec Canada
Symantec™ Global Intelligence Network
Identifies more threats, takes action faster & prevents impact

Worldwide Coverage
Global Scope and Scale
24x7 Event Logging

Rapid Detection

Attack Activity
- 240,000 sensors
- 200+ countries and territories

Malware Intelligence
- 180M client, server, gateways monitored
- Global coverage

Vulnerabilities
- 50,000+ vulnerabilities
- 15,000+ vendors
- 105,000+ technologies

Spam/Phishing
- 5M+ decoy accounts
- 8B+ email messages/day
- 1B+ web requests/day

Preemptive Security Alerts
Information Protection
Threat Triggered Actions

Best Practices for a BYOD World SecTOR 2012
Mobile Threats Expose Organizations and Consumers
Mobile Malware on the Rise

- This represents families of mobile malware
- There are 3,000-4,000 variants in the wild today and growing

Source: Symantec
Mobile Threats Focus Areas for Malware Authors

- Stealing information, spying and sending SMS messages
- Malware authors porting old threats and working on new ones
- Most popular way to make money? Sending premium SMS
Mobile Device Explosion Paves Way for BYOD

- 2010: 177M corp PCs; 2015: 246M corp PCs (39% increase)
- 2010: 173M personal PCs; 2015: 293M personal PCs (69% increase)
- 2010: 300M smartphones; 2015: 1017M smartphones (340% increase)
- 2010: 15M tablets; 2015: 326M tablets (2,170% increase)
Corporate Computing in Transition

- New generation of app-centric devices emerged
- BYOD and employee-liable device trend accelerating
- New generation of mobile corporate apps being deployed
- Co-mingled business / personal data on all devices

By 2014, 90% of organizations will support corporate applications on personal devices*

By 2013, 80% of businesses will support a workforce using tablets*

*Source: Gartner, Inc.; Gartner’s Top Predictions for IT Organizations and Users, 2011 and Beyond: IT’s Growing Transparency – Summary Report; Nov 30, 2010
No Conventional Control ...

“No organisation can afford to fix an unlimited range of issues on a large portfolio of devices, many of which the organisation doesn't own and therefore can't control in conventional ways.”

Gartner, July 2011
Mastering Mobile Control Points

Devices

Apps

Data

...without disrupting user experience
Consumerization is Driving BYOD

Unmanaged

Company Owned But Unmanaged

Managed

Traditional Focus

Company Controls Standard Device

Company-owned

Personally-owned

Evolving Focus

Company Controls Relevant Apps & Data Only

Company Controls Personal Device

Best Practices for a BYOD World SecTOR 2012
It doesn’t matter where the information is... !!!
Mobile Phones/Devices: A New Source of Data Breaches

- Mobile devices contain work and personal information
- Unlike a desktop computer they are easily stolen
- ... and often lost
Honey Stick Project: Smartphone Edition
Only 50% of finders attempted to return the phones.
96% of all phones had personal & business apps accessed
Best Practices for BYOD
## Mitigating Mobile Threats

<table>
<thead>
<tr>
<th>Category</th>
<th>Recommendations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Management</strong></td>
<td>- Remotely wipe devices in case of theft or loss</td>
</tr>
<tr>
<td></td>
<td>- Update devices with applications as needed without physical access</td>
</tr>
<tr>
<td></td>
<td>- Get visibility and control of devices, users and applications</td>
</tr>
<tr>
<td><strong>Device Security</strong></td>
<td>- Guard mobile device against malware and spam</td>
</tr>
<tr>
<td></td>
<td>- Prevent the device from becoming a vulnerability</td>
</tr>
<tr>
<td></td>
<td>- Enforce compliance across organization, including security standards &amp; passwords</td>
</tr>
<tr>
<td><strong>Content Security</strong></td>
<td>- Identify confidential data on mobile devices and use technologies to prevent future exposure</td>
</tr>
<tr>
<td></td>
<td>- Protect data from moving between applications</td>
</tr>
<tr>
<td></td>
<td>- Encrypt mobile devices to prevent lost devices from turning into lost confidential data</td>
</tr>
<tr>
<td><strong>Identity and Access</strong></td>
<td>- Provide strong authentication and authorization for access to enterprise applications and resources</td>
</tr>
<tr>
<td></td>
<td>- Ensure safe access to enterprise resources from right devices with right postures</td>
</tr>
</tbody>
</table>
**Best Practices for BYOD**

| **Assess** | • Assess threats, conduct a risk analysis, run a policy audit and an apps audit, evaluate architectural planning and security. |
| **Data Classification** | • Determine what sensitive information exists in your organization  
  • Categorize it appropriately and protect it according to its classification level |
| **Encryption** | • Create and enforce security policies so all confidential information is encrypted |
| **Data Loss Prevention** | • Discover data spills of confidential information.  
  • Detect and prevent exfiltration of confidential information |
| **Security Awareness Training** | • Ensure employees become the first line of defense against socially engineered attacks, such as phishing, spear phishing, and other types of attacks |
BYOD Success Mantra...

• Enable broadly

• Think strategically

• Manage efficiently

• Enforce appropriately

• Secure comprehensively
Stay Informed

Symantec Intelligence
Internet Security Threat Report
BUILD YOUR REPORT

Security Response Website

Symantec Security Response
Our security research centers around the world provide unparalleled analysis of and protection from IT security threats that include malware, security risks, vulnerabilities, and spam.

Monthly update URL

www.symantec.com/threatreport

@SymantecCanada
@Threatintel

Best Practices for a BYOD World SecTOR 2012
Thank you!

Sangameswaran Manikkayam Iyer
MV_Sangameswaran@symantec.com