A GLOBAL POWERHOUSE IN BUSINESS AND IT TRANSFORMATION

WHO WE ARE

93,000	EMPLOYEES OPERATING IN 70 COUNTRIES
#162	RANKING ON THE FORTUNE 500 FOR 2012
$15.5B	GLOBAL IT SERVICES POWERHOUSE
50+	YEARS OF INNOVATION
100+	GLOBAL ALLIANCES WITH BEST-IN-BREED PARTNERS

CSC GLOBAL CYBERSECURITY

A LEADER AND INNOVATOR IN FULL LIFECYCLE SECURITY DELIVERY

WHO WE ARE

1,700+	GLOBAL CYBERSECURITY PROFESSIONALS
250+	GLOBAL CYBERSECURITY CLIENTS
5+	INTEGRATED GLOBAL SECURITY OPERATIONS CENTERS
20+	YEARS EXPERIENCE IN SECURITY OUTSOURCING, CONSULTING AND INTEGRATION
15+	GLOBAL ALLIANCE PARTNERS PROVIDING SECURITY EXPERTISE

Questions…

- Do you have BYOD in your organization?
- How may endpoints do you have?
- What information is stored on them?
- Where are they located?

BYOD Statistics

- Whether you have an official BYOD policy or not, chances are your employees are using personally owned devices for business purposes.
- 67% of knowledge workers and 57% of other works use one or more personal devices for work at least once a day.
- Daily personal use by type of device:
  - 47% of standard phone owners
  - 43% of smartphone owners
  - 39% of desktop owners
  - 35% of laptop owners
  - 17% of tablet users

Source: Gartner Market Trends: How BYOD Impacts Teleworking and Workplace Usage, Mikako Kitagawa, 25 March 2013.

Why do employees BYOD anyway?

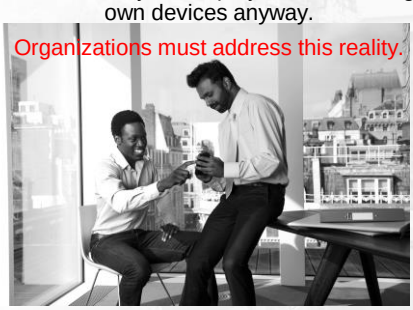
- Some provide a work device that is not supplied by their employer
- 57% of knowledge workers who are provided with laptops by their employer still report using their own laptop for work every day
- Emerging markets: Compensation for lack of IT Infrastructure
- USA: Highest allocation of working hours at home – less clear boundaries

Source: Gartner Market Trends: How BYOD Impacts Teleworking and Workplace Usage, Mikako Kitagawa, 25 March 2013.

Reality check:

The fact that you don't have a BYOD program doesn't mean that your employees aren't using their own devices anyway.

Organizations must address this reality.



What are the security issues?

- Company data on a device the company doesn't own
  - Data ownership issues
  - Confidentiality and integrity controls
  - Retention, archival, legal, and regulatory issues
- Personal device controlled by company?
  - Liability, personal privacy
- Communication paths may bypass enterprise controls
  - Malware vector
  - DLP, monitoring, archival

BYOD Laptops

- How can we achieve standardized controls?
  - Antivirus / Antimalware
  - Firewall
  - DLP
  - Hard drive encryption
  - Backups
  - ….
- How much corporate data remains on personal laptops?
  - Primary storage? Secondary? Artefacts?

Mobile Phones and Tablets

- All the risks associated with a laptop plus…
  - Easier to lose or have stolen
  - Additional users (family members)
  - Increased connectivity (WiFi, Bluetooth, Wireless Carrier)
  - Roam in and out of the corporate security perimeter (if one really exists today)

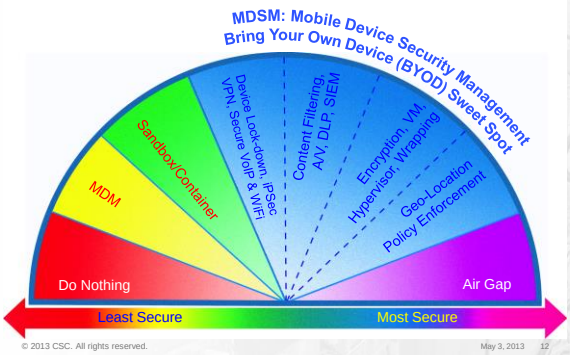
BYOD is not a Binary Decision

- BYOD is here to stay, but some limits are appropriate
- Some functionality impacts the enterprise less than others
- Different levels of management are available
- Winn Schwartau, author and Chairman of Mobile Active Defence proposes viewing BYOD mobile security as a spectrum:

Source: Mobile Active Defence, The BYOD Mobile Security Spectrum, Winn Schwartau, July 1, 2012. http://www.mobileactivedefense.com/wp-content/uploads/2010/10/The-BYOD-Mobile-Security-Spectrum-July_1_2012FINAL.pdf

BYOD Mobile Security Spectrum

Courtesy of Winn Schwartau, Mobile Active Defense



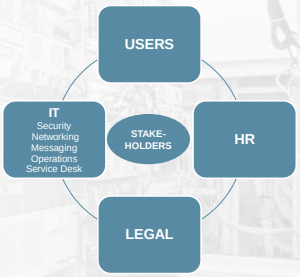
Managing BYOD: A Practical Approach

- Take a risk-based approach – protect what matters
- Align BYOD policy with information classification policy and handling standards
- Consider human behaviour and motivation as well as security goals
  - Why are employees using their own devices?
  - Are we supplying them appropriate equipment?
  - Are their cost-effective ways to reduce to risk?
  - Does anybody really want this?

Managing BYOD: 3 Core Elements

Policy and Governance

- Clearly articulate responsibility and ownership of company data
- Address liability for personal information
- Are we protecting data based upon it's sensitivity, or some other criteria?



Policy and Governance

- Clearly articulate responsibility and ownership of company data
- Address liability for personal information
- Are we protecting data based upon it's sensitivity, or some other criteria?
- Processes:
  - Enrollment in program
  - Technical support
  - Inventory/Approval Process
  - Lost devices and employee termination
  - e-discovery and investigations

Awareness Training

- Include BYOD issues in enterprise security awareness training.
- Policy and technical controls don't work if users don't understand the need to protect information
- Users will bypass inconvenient controls. User-initiated BYOD may be a symptom of another problem.
- To succeed we must influence behaviour.
- Leverage training sessions to obtain feedback on what works and what doesn't.

Technical Controls

- Various levels of control are available for mobile devices:
  - No management
  - Device security policy enforcement (MDM)
  - Compartmentalization of corporate data
  - VPN (demand, always-on, split?)
  - Leveraging VPN for content filtering and policy enforcement
  - Geo-location policy management
- Controls should be dictated by an assessment of risks
- Consider virtual desktops?

Questions?

Eric Jacksch
+1-613-454-8200
ejacksch@csc.com

http://www.csc.com/cybersecurity