

Cyber CYA Webinar Series:

# Policies for Personal Use, Managing Devices on Your Network

CYBER: CYA   
Education to Cover Your Assets

  
TECHSOURCE

THE PIKES PEAK SMALL BUSINESS DEVELOPMENT CENTER HAS BEEN DEDICATED TO HELPING EXISTING AND NEW BUSINESSES GROW AND PROSPER FOR MORE THAN 30 YEARS.



FREE  
CONSULTING



PRACTICAL  
TRAINING



BUSINESS  
RESOURCES



Funded in part through a cooperative agreement with the U.S. Small Business Administration

[WWW.PIKESPEAKSBDC.ORG/CONSULTING](http://WWW.PIKESPEAKSBDC.ORG/CONSULTING)

[WWW.PIKESPEAKSBDC.ORG/WORKSHOPS](http://WWW.PIKESPEAKSBDC.ORG/WORKSHOPS)

*Cyber CYA Series: Policies for Personal Use  
Devices on Your Network*



# **Bring Your Own Device (BYOD)**

Increased Productivity, Increased Risk, The Balancing Act

*Dr. Shawn P. Murray, C/CISO, CISSP, CRISC  
October 10, 2019*

# BYOD

## Agenda

- BYOD – Defined
- Evolution of BYOD
- Advantages of BYOD
- Case Studies
- **Risks and Threats**
- **Case Studies**
- **CIA**
- **Data Breach**
- **Configuration Management**





## A Brief Evolution of BYOD (BYOD Defined)

- 2009 The Term BYOD Emerges by Intel Corporation
- 2010 - IT Can't Ignore Personal Devices
- 2011 - BYOD is Here to Stay
- 2012 - Data Security Takes Centre Stage
- 2013 - The App Explosion
- 2014 - BYOD Ceases to Exist

*"In 2014, BYOD evolved to become more about enablement and corporate access that goes beyond email. Employees expect the same access to workplace content on their mobile devices that they have on their laptops and PCs. MDM and MAM have shifted to EMM, as the industry evolves to cater to a broader set of mobile capabilities for the enterprise based on use cases across users, devices, apps and content."*

*"BYOD has ceased to exist, and has been replaced by a broader set of mobile capabilities that enable the workforce of the future. BYOD is morphing into BYOx – a*

## Advantages & Perceptions

A study by IBM says that 82% of employees think that smartphones play a critical role in business.

The study also shows benefits of BYOD include:

- **Increased productivity** - Increased productivity comes from a user being more comfortable with their personal device; being an expert user makes navigating the device easier, increasing productivity.
- **Cost savings for the Company** - Cost savings can occur on the company end because they now would not be responsible for furnishing the employee with a device, but is not a guarantee.
- **Employee satisfaction** - Employee satisfaction, or job satisfaction, occurs with BYOD by allowing the user to use the device they have selected as their own rather than one selected by the IT team. It also allows them to carry one device as opposed to one for work and one

A Gartner strategic planning assumption indicates “by 2020, 85% of organizations will adopt BYOD in some form.”

## No turning back

Shows that the primary benefits of BYOD programs are improved employee mobility (57%), Greater employee satisfaction (56%)

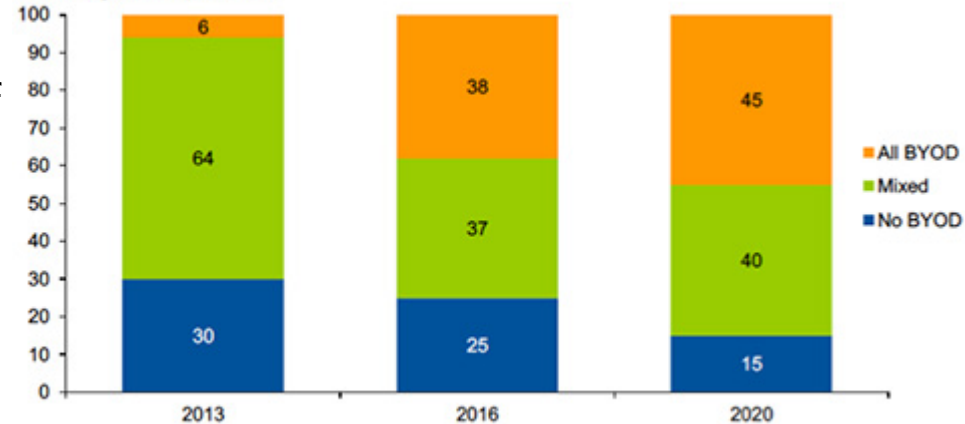
Improved productivity (54%).

The same survey indicates the biggest security concerns are loss of company or client data (67%), Unauthorized access to company data and systems (57%)

Users downloaded apps or

Q. When will your organization cease to provide personal devices?

Percentage of Respondents



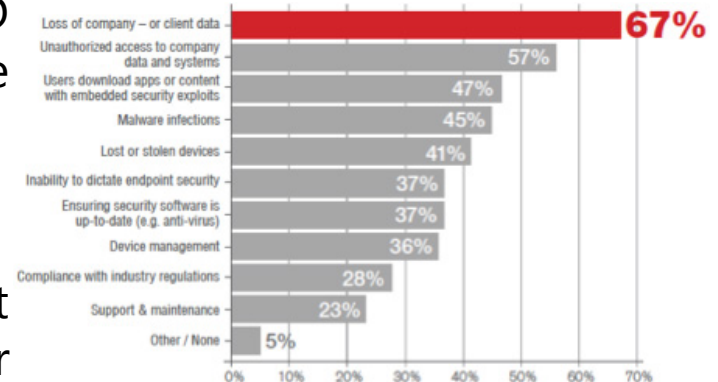
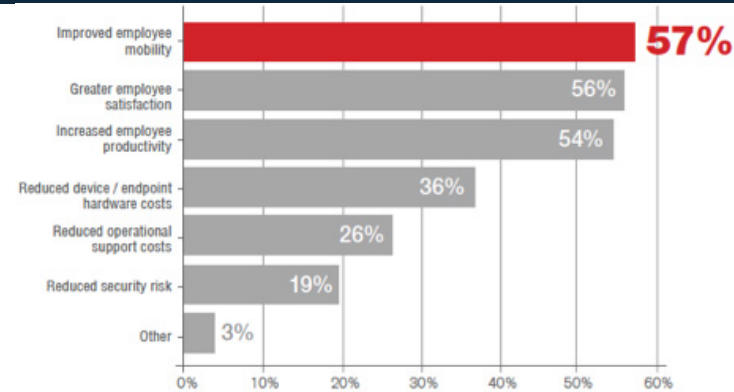
N = 2,206 worldwide



# BYOD and Mobile Security Survey by the Information Security Group

## *A recent survey about BYOD and Mobile Security by the Information Security Group on LinkedIn*

- Shows that the primary benefits of BYOD programs are improved employee mobility (57%),
- Greater employee satisfaction (56%)
- Improved productivity (54%).
- The same survey indicates the biggest security concerns are loss of company or client data (67%).





# Heartbleed Attack on BYOD Service Hit Insurance Giant Aviva



Heartbleed vulnerability was leveraged in an attack against a BYOD service provider

- Allowing the attackers to potentially cause millions in damages for insurance giant Aviva
- A number of the company's fleet of employee-owned mobile devices were wiped clean.
- "Aviva was using BYOD service MobileIron to manage more than 1,000 smart devices such as iPhones and iPads.
- On the evening of the 20 May 2014, a hacker compromised the MobileIron admin server and posted a message to those handhelds and the email accounts, according to our source," the report stated. "The hacker then performed a full wipe of

# 6 Biggest Business Security Risks and How You Can Fight Back - CIO Magazine

IT and security experts discuss the leading causes of security breaches and what your organization can do to reduce them.

- Risk No. 1: Disgruntled Employees
- Risk No. 2: Careless or Uninformed Employees
- **Risk No. 3: Mobile Devices (BYOD)** "Data theft is at high vulnerability when employees are using mobile devices [particularly their own] to share data, access company information, or neglect to change mobile passwords," explains Jason Cook, CTO & vice president of Security, BT Americas. "According to a BT study, mobile security breaches have affected more than two-thirds (68 percent) of global organizations in the last 12 months."

**2015 Mobile Security Survival Guide -**

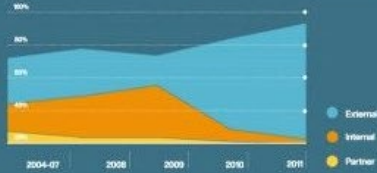
# BYOD – Data Breaches

## Data security breaches: figures are shocking

**INSIGHT**  
 Staff using their own technology at work highlights the role of employees in information security - or the lack of it, writes Rod Newing



Data breaches in business worldwide



Current and projected percentages of mobile device users with single and multiple devices worldwide



Compromised records by type of threat worldwide, 2004-11



Average past and projected growth in mobile device connectivity rates worldwide



Cyber attacks by month, method, motivation and target worldwide, 2012 (%)



# What do you need to consider in your BYOD Policy?

- Application Security (include 3<sup>rd</sup> party)
- Sensitive Data Access
- Loss of Devices
- Sold or disposed without sanitizing
- Malware
- Vulnerability Management
- Confiscation for Incident Response
- Conflict with other policies



# Mobile Security Reference Architecture

- The figures for using mobile devices for work related tasks in 2016 are estimated at 350 million users of mobile devices, of which 200 million will be using their own personal devices for work-related tasks as well it is expected that this number will double by 2020.
- The MSRA document provides reference architecture for mobile computing, released by the Federal CIO Council and the Department of Homeland Security (DHS) to assist Federal Departments and Agencies (D/As) in the secure implementation of mobile solutions through their enterprise architectures. One important assumption pointed out by the council is that this reference only applicable to mobile devices including mobile phone and tablet, but not laptops and other

# BYOD – Instituting Controls (MDAC)



## ***Implement Mobile Device Access Control (MDAC).***

- Designed to control network access and bandwidth for employee-owned mobile devices, including Smartphones and tablets.
- Goes beyond password protection by preventing network access until the devices comply with a pre-established list of criteria.
- Typically includes a certain anti-virus protection level and having the most recent system updates and patches.
- With MDAC, organizations also can redirect users to self-registration portals, block usage of certain applications and control bandwidth usage by the type of device.



# BYOD – Instituting Controls (MDM issues)



## **Mobile Device Management (MDM)**

*“While MDM provides organizations with the ability to control applications and content on the device, research has revealed controversy related to employee privacy and usability issues that lead to resistance in some organizations.”*


*“Corporate liability issues have also emerged when businesses wipe devices after employees leave the organization.”*

### Issues Include:

- Who owns the telephone number

- Separating personal content from company data - being monitored

- Misuse of corporate access on personal devices



**Thank You!**  
**Open Discussion**  
**QUESTIONS?**

# References & Resources

International Journal of Mobile Network Communications & Telematics ( IJMNCT) Vol. 4, No.5,October 2014

**Detecting cyber attacks in a mobile and BYOD organization** by Oliver Tavakoli

CTO at Vectra Networks - Tuesday, 14 October 2014.

A Brief History of BYOD and Why it Doesn't Actually Exist Anymore, By James Laird on 07 Nov 2014

<http://searchmobilecomputing.techtarget.com/tip/Minimizing-BYOD-security-risks-through-policy-and-technology>



# Pikes Peak Small Business Development Center

559 E. Pikes Peak Ave., Suite 101, Colorado Springs, CO 80903

719-667-3803  
[sbdc@elpasoco.com](mailto:sbdc@elpasoco.com)

[www.pikespeaksbdc.org](http://www.pikespeaksbdc.org)

## OUR SPONSORS:



*Funded in part through a cooperative agreement with the U.S. Small Business Administration*