

BYOD



Presented by:
Robin Fowler, CBE, ACE, CMO, CMFF
Certified Forensic Examiner



BYOD

- What is BYOD?
- History of BYOD
- Advantages and Disadvantages
- Mitigating the risks



What is BYOD anyways?

- BYOD or Bring Your Own Device
- Related acronyms include:
 - BOYT (Bring Your Own Technology)
 - CYOD (Choose your Own Device)



What is BYOD anyways?

The Past



What is BYOD anyways?

The present



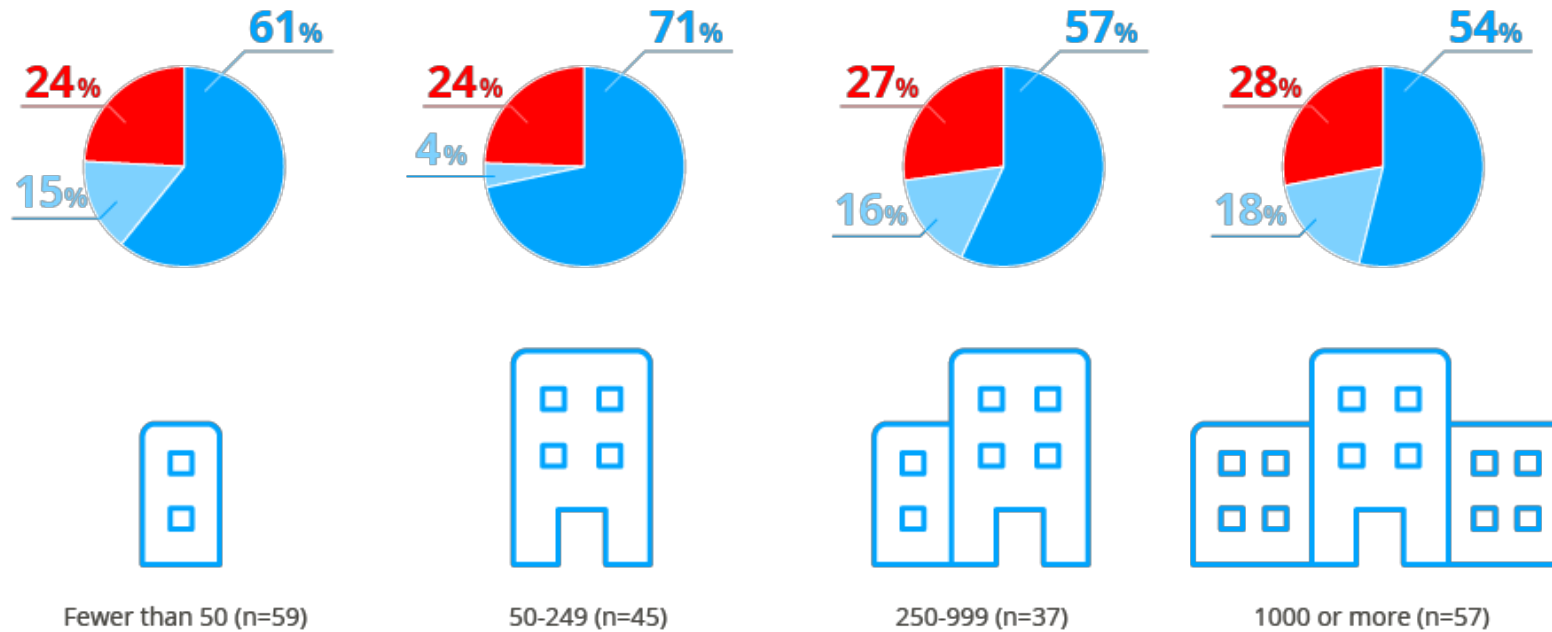
History of BYOD




- Intel embraced the BYOD concept in 2009
- Gained mainstream adoption and promotion from Citrix and Unisys
- Over half of all companies small or large now have BYOD in place



History of BYOD

BYOD Usage by Company Size



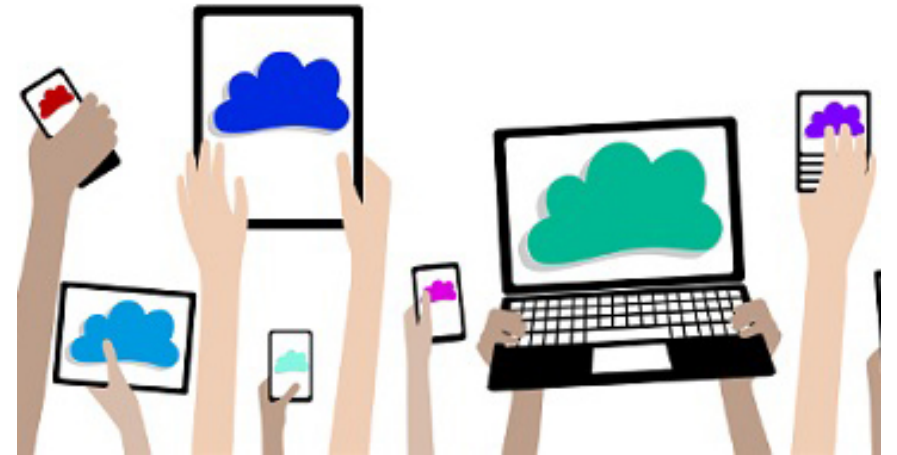
-  Yes, we currently allow the use of personal devices for work purposes (i.e., access company networks and data)
-  We do not currently allow, but within the next 12 months we plan to begin allowing the use of personal devices for work purposes
-  No, we have no plans to allow the use of personal devices for work purposes

n=Number of respondents



Advantages

- Productivity Gain
- Increased Morale
- Cost Savings
- Faster Technology Upgrades



Productivity Gains

- Employees tend to be more productive
- More likely to make use of devices they are comfortable with
- All important information contained on one device



Increased Morale

- Better Work Life Balance
- Devices they are familiar with
- Flexibility



Cost Savings

- Shifting costs
- Lower Hardware costs
- Lower Data plan costs



Faster Technology Upgrades

- Employees upgrade more often
- Newer devices offer better security



Pitfalls to Avoid

- Data leakage/Data breach
- Malware and Virus
- Lack of device management
- Lack of testing



Data Leakage

The risk of Data Leakage can be minimized by the proper use of:

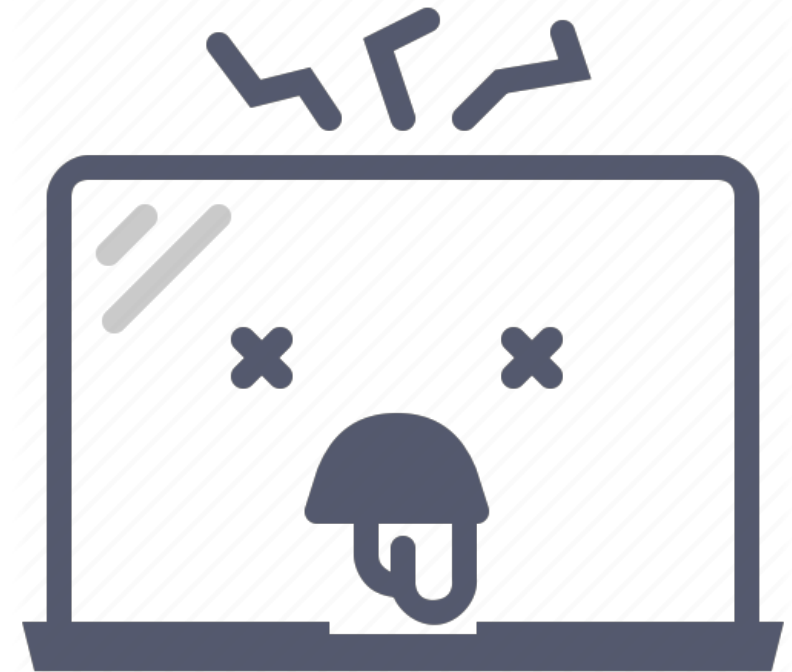
- Mobile device management
- Data provisioning
- VPN or App segregation
- Geo location



Malware and Virus

The risk of malware and virus threats can be minimized by:

- App permission auditing
- Ensuring all devices are updated
- App blacklists



Device management

Device management can assist in securing BOYD devices by:

- Mobile data wiping
- On device data security
- Monitoring and tracking of devices



Penetration Testing

Penetration testing is the act of examining the security of your system

- Will uncover vulnerabilities so they can be patched before bad actors exploit them
- Should be performed on a regular basis
- Discuss with your cybersecurity provider



Takeaways

BYOD can be a great resource for your company to leverage employee engagement and morale. Ensure a robust Mobile Device Management plan is in place that includes the following to minimize the risk of data loss:

- Data breach/Leakage protection
- Application permission reviews
- Application blacklisting
- Mobile data wiping
- Device monitoring and tracking
- Penetration test your security often



Questions?

