BYOD Policies &ndash; More than an IT Issue Part 4: User Experience and Privacy

Peter Silva, 2012-22-10

#BYOD or Bring Your Own Device has moved from trend to an permanent fixture in today's corporate IT infrastructure. It is not strictly an IT issue however. Many groups within an organization need to be involved as they grapple with the risk of mixing personal devices with sensitive information. In my opinion, BYOD follows the classic Freedom vs. Control dilemma. The freedom for user to choose and use their desired device of choice verses an organization's responsibility to protect and control access to sensitive resources. While not having all the answers, this mini-series tries to ask many the questions that any organization needs to answer before embarking on a BYOD journey.

Enterprises should plan for rather than inherit BYOD. BYOD policies must span the entire organization but serve two purposes - IT and the employees. The policy must serve IT to secure the corporate data and minimize the cost of implementation and enforcement. At the same time, the policy must serve the employees to preserve the native user experience, keep pace with innovation and respect the user's privacy. A sustainable policy should include a clear BOYD plan to employees including standards on the acceptable types and mobile operating systems along with a support policy showing the process of how the device is managed and operated.

Some key policy issue areas include: Liability, Device Choice, Economics, User Experience & Privacy and a trust Model. Today we look at User Experience & Privacy.

User Experience and Privacy

Most application deployments have the user experience in mind and BYOD is no different. Employees want and need fast and secure access to the right resources, at the right time to accomplish their job. BYOD only enhances or increases the need for a rich user experience. Understand how the policy impacts user experience including battery life. Some apps can drain battery life quickly, which in turn decreases user satisfaction and can potentially limit their interactions. There may be instances where the user has chosen a third-party email application verses either the native email client or one that's supported by corporate. Certainly a dilemma but as stated earlier, a policy should state what's allowed and not allowed. MDM technology is also improving to the point that Secure apps like a browser, email client and other resources are secured on the client device. A user can still use their email client of choice for personal use but work email is delivered through the secure email client.

While user experience can contribute to the happiness and productivity of the user/employee, privacy can be a huge issue when BYOD is implemented. A 2010 Supreme Court case, *City of Ontario v. Quon*, looked at the extent to which the right to privacy applies to electronic communications in a government workplaces. This case also looked at Fourth Amendment rights against unreasonable search and seizure. Essentially, a number of police officers were fired for sending sexually explicit message with a city issued device. The city requested an audit of the overages along with the sent messages. The officers sued since the agreement/policy they had with the city allowed them to send personal notes and pay for any overages that might occur. Plus they claimed that their constitutional right was violated along with their privacy under federal communications laws. The court ruled that since they were using city issued devices, the municipality was well within their rights to search since it was work related and it had not violated the Fourth Amendment. If everything was the same but the devices were personally owned by the officers in question, then the city could be in violation and liable.

Within the BYOD policy, organizations should also establish a social contract that communicates how and when IT will monitor the device along with when/how/why a device could be wiped.

As part of the BYOD Policy the User Experience & Privacy Checklist, while not inclusive, should:

· Identify what activities and data must be monitored

· Determine the circumstances when a device wipe must occur

· Determine how employees can self-remediate

· Determine which core services will be delivered to users

· Draft a BYOD social contract with Human Resources

ps

Related

- BYOD Policies – More than an IT Issue Part 1: Liability
- BYOD Policies – More than an IT Issue Part 2: Device Choice
- BYOD Policies – More than an IT Issue Part 3: Economics
- BYOD–The Hottest Trend or Just the Hottest Term
- FBI warns users of mobile malware
- Will BYOL Cripple BYOD?
- Freedom vs. Control
- What’s in Your Smartphone?
- Worldwide smartphone user base hits 1 billion
- SmartTV, Smartphones and Fill-in-the-Blank Employees
- Evolving (or not) with Our Devices
- The New Wallet: Is it Dumb to Carry a Smartphone?
- Bait Phone
- BIG-IP Edge Client 2.0.2 for Android
- BIG-IP Edge Client v1.0.4 for iOS
- New Security Threat at Work: Bring-Your-Own-Network
- Legal and Technical BYOD Pitfalls Highlighted at RSA