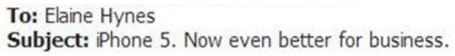
THOUGHT LEADERSHIP @ KS&R

It’s 9:00 am:

Do you know what devices your employees are using?

By Elaine Hynes, Director of Strategic Analysis, KS&R

Recently, this came into my inbox:



To: Elaine Hynes
Subject: iPhone 5. Now even better for business.

I see ads like this every day. I’m not surprised I’m being marketed to this way – almost everyone I know uses their personal mobile technology devices for work-related purposes. But for many companies, not knowing how many employees are using which devices and for what, can be a major liability.

To Allow Or Not to Allow – Is That Even The Question?

For most of our clients, including those who work in large, enterprise organizations, Bring Your Own Device – or BYOD – isn’t a phenomenon that can, or should, be stopped. Whether it’s a smartphone, a tablet, or a laptop, employees are already using them for work. Most companies are encouraging their use, citing benefits such as:

- Greater productivity
- Increased connectivity
- Better cost-control, especially for companies with mobile workforces

On the flip side, however, there can be negatives. If your business employment status makes you qualified for litigation (e.g., if you’re a CEO, director, etc.), using your personal mobile device at work may have unintended consequences of a legal nature, as in the case of pre-trial discovery, where personal data, along with company data, could be exposed.

In addition to legal issues, you also need to consider whether:

- BYODs are compatible with your current IT capabilities
- Using BYODs compromises your corporate data’s security
- Employees have an understanding that some of their personal data may become public if they are involved in litigation

For example, if company data is subpoenaed, will all the data on the CEO’s iPhone become public? If an employee logs into the company network to view HR records at home, can someone outside the company gain access that private information as well?

The best course of action is to put a BYOD corporate policy in place that regulates what devices employees are allowed to use, and which data is accessible on those devices. But before companies put a policy in place they have to know more about what technologies their employees are bringing into work, and how they’re using them.

How Research Can Help

A survey on employee devices can be a standalone entity, or part of a broader employee survey. The survey questions need to get to the heart of employees’ BYOD usage and capture work-related device information, including:

- The number of people who are currently using their own mobile technology devices
- How many people are planning to use devices in the future
- What types of devices are people using (smartphones, tablets, laptops)
- The capabilities of the devices people are using (text, email, web)
- Tasks that employees are using their devices for
- The types of corporate data

ABOUT THE AUTHOR

Elaine Hynes is KS&R’s Director of Strategic Analysis, and has lead a wide variety of business (B2B) and consumer (B2C) research projects, both qualitative and quantitative (statistical) in nature.

employees are accessing with mobile devices

- Amenability to certain scenarios (e.g., *"If you could only use your personal devices for some specified work activities, but not others, would you still use your device at work?"*)
- How employees would like to use their devices in the future, such as what data they'd like to access, or tasks they'd like to perform
- Whether employees expect to be compensated at all, or in part, for their device and/or service fees

Using the Data to Construct a Policy

Once the data has been gathered, it will serve as the basis for writing a BYOD policy that can be implemented companywide. After a policy is firmly in place and communicated throughout the company, implementation can then begin, involving not only IT, but HR, legal, and strategic planning.

That policy should ideally include:

1. Which mobile devices will/will not be supported corporately. Knowing what devices most people already own can help companies determine which devices will be supported by the company.
2. Guidelines about who pays and how much. When you understand the extent of your employees BYOD usage, including what they are paying for their plans, you can determine whether or not you will pay for devices in whole or in part, or reimburse employees for service fees, or implement any other subsidization program.
3. Access rules. During research, you may discover that employees are accessing data that may compromise security – or, they may want to access information that's not yet available. Having this information will help you craft a policy and weigh the technical issues regarding applications, services and data employees can use, which will be denied and which have conditional access based on job function or title.
4. Security procedures. As employees access more data online, a corporate policy will need to include and communicate a procedure to manage activities required for security of both corporate and personal data, such as passwords, anti-malware software, encryption, etc.
5. Personal information privacy parameters. In addition to compliance with privacy legislation, corporations will need to determine what types of private information corporate applications or services will NOT be allowed to access on personal devices.
6. Written employee BYOD usage agreement. Corporate BYOD activity should lead to an extension of the standard practice of asking new hires to sign an "acceptable usage policy" agreement before being given access to IT resources. The BYOD usage agreement should clearly document what users are, and are not, allowed to do with their mobile devices within the company. If sanctions are going to be implemented if the employee's actions contradict the agreement, these must be clearly articulated within the agreement.

The Bottom Line: Know What's Happening in Your Company

With millions of people bringing their personal mobile technology devices to work, BYOD is increasing productivity, but can also lead to adverse events such as privacy issues, IT headaches and security concerns. The best course of action is to get an accurate initial baseline and subsequent periodic updates of the BYOD situation in your company, and craft and maintain a policy that keeps the productivity and protects you from potentially damaging outcomes.

So, I'll go back to my initial question: ***It's 9:00 am. Do you know what devices your employees are using?***