P&N
Postlethwaite & Netterville

BYOD: Cybersecurity in a Bring Your Own Device World

by Michael Richmond

It’s a fact: the development of technology dramatically outpaces the development of policies and controls that mitigate the risks of technological advances. In common terms: it’s only once a new technology is developed (or adopted) that we figure out all the bad things that can happen with that technology, and we put rules and other controls in place to keep those bad things from happening. Case in point: BYOD.

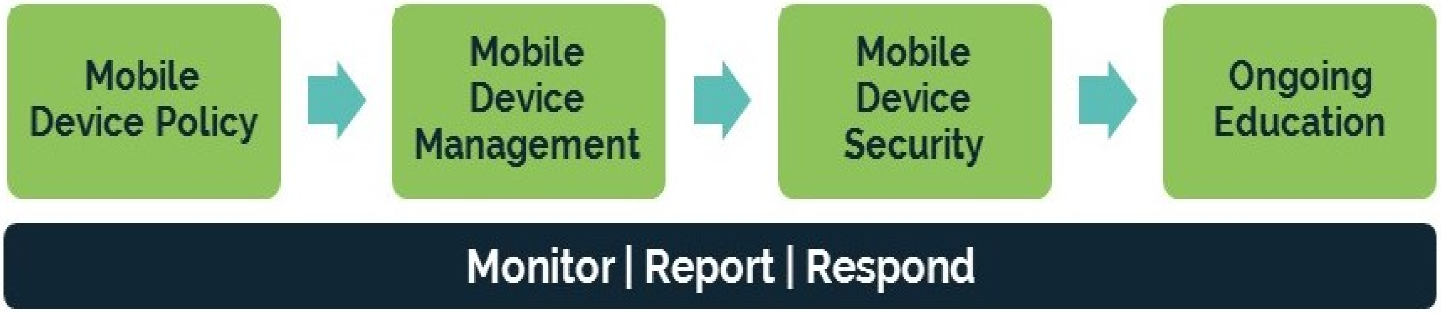
BYOD (Bring Your Own Device) is the policy of allowing employees to use personally-owned devices such as mobile phones, tablets, and laptops, to access company-owned information and applications.

A 2017 Cisco study found that almost 70% of IT decision makers were in favor of BYOD policies, and their reasoning is sound. First, allowing employees to use their own devices can result in cost savings through reduced hardware costs for mobile devices. For example, assume a company has 100 employees who need remote access to work applications. Even at a conservative $500 per mobile device, the company could save $50,000 in hardware costs by allowing those employees to use their own devices.

And allowing employees to use their own devices is generally what they prefer. Multiple employee surveys and studies have shown that employees prefer using their own devices for a variety of reasons. It’s more convenient than carrying around multiple devices; it allows for better work-life integration; it allows team members to select the device they prefer; and it increases productivity by giving the employees a single device to manage and learn to use.

When you consider the potential cost savings, increased productivity, and greater employee morale, it’s not surprising that so many IT decision makers support BYOD policies. However, allowing foreign devices to access corporate applications and data does not come without risks, and as BYOD continues to grow in popularity, so does the potential for cyber criminals to utilize weak cybersecurity protocols to gain access to company systems.

If your company allows (or is considering) BYOD, having a layered approach to mobile device management is critical. Consider these risks and tips to mitigate them.



Mobile Device Policy
It's not just words on paper. Having a robust mobile device policy defines the "rules" of allowing employees to access company resources. This is where you spell out which applications are accessible, how you will monitor usage, how employees are expected to protect their devices, the usage of passcodes, and other policies that protect your company.
This is also where you define what happens if an employee leaves your company. How will you ensure continued protection for your data and systems through a device that you don't own?
Tip: Make the policy mandatory, ensure that it is legal and enforceable, communicate it to all users, and require signatures.

Mobile Device Management
Once you have established (and communicated) the rules of BYOD, the next layer focuses on allowing your company to manage the data and applications the device has access to. Mobile device management software allows you to containerize your data, so that you can allow access through mobile devices, but also retrieve access when needed. Consider how you would respond if a device is lost or stolen, or when an employee terminates employment. Your written policy may allow you to wipe the device, but this layer provides you with the tools to actually do it.
Tip: Employ mobile device management software to allow you to remotely "wipe" company data quickly in case of lost or stolen devices, employee termination, or other security issues.

Mobile Device Security
On top of the layers of written policy and mobile device management tools comes data security. Mobile device security helps prevent exposing corporate data through usage of mobile devices. This includes identity and access management, VPN, endpoint security, firewalls, gateways, cloud access security brokers, and other security measures aimed at preventing unauthorized access to data from mobile devices.

Tip: Solutions for mobile device security are complex. Proper security architecture is critical, and has applications and impacts beyond BYOD. Security protocols can be leveraged for any remote accessibility, including company-owned mobile devices and laptops.

Employee Education
Like we mentioned in our article on Phishing & Employee Education, one of the weakest links in any company's cybersecurity effort is its employees. This is especially true with mobile, employee-owned devices. They control the device, they generate the data, and they are responsible for the physical security of it. Helping them make smart decisions when accessing data or managing their device is absolutely critical.

Tip: Employee education is not a one-and-done initiative. It should be a constant focus through a comprehensive training and education plan.

Monitor, Report, & Respond
Finally, monitoring, reporting, and responding to mobile device issues (and all cybersecurity issues) should be embedded throughout your BYOD plan. You can't respond to issues if you don't know about them, you can't know about issues if you don't report, and you can't report if you don't monitor. Knowing who is accessing your data, how they are accessing it, and what they are doing with it allows your team greater insight into your vulnerabilities.

Tip: Don’t just watch and wait. Be aggressive with your cybersecurity protocols by conducting periodic vulnerability testing. If you aren’t finding (and fixing) the vulnerable access points, cyber criminals will.

For more information on mobile device management and other cybersecurity services, contact our Technology Services Group.