Use Bring-Your-Own-Device Programs Securely

By Dale Gonzalez
December 2012

Bring-your-own-device (BYOD) programs, which allow employees to use their personal smartphones, tablets and laptops in and out of the work environment, are changing the IT landscape. Organizations around the world are embracing BYOD, because it allows executives and employees to use the mobile devices, service providers and operating platforms of their choice.

IT research analysts at Gartner, Inc. predict 90 percent of organizations will deploy corporate applications on personal devices by 2014 (See, “Gartner Reveals Top Predictions for IT Organizations and Users for 2011 and Beyond,” Gartner.com, http://gtnr.it/gUFPRk) BYOD allows employees to be more productive and conduct business activities outside of traditional working hours. But just as there are considerable benefits, there are information security concerns for all organizations.

Considerations before implementing BYOD

Threat actors such as cybercriminals, hackers, and hactivists are increasingly turning their focus to small businesses because they typically lack the breadth of security measures prevalent in larger organizations. Threat actors are after money, sensitive customer and employee data, patent information, trade secrets, and even access to your business partners. BYOD, if not used securely, potentially opens one more window of opportunity for threat actors.

Additionally, most organizations are subject to federal, state and/or industry regulations regarding information security safeguards. The choices you make regarding BYOD can impact your ability to comply with regulations. If your organization and/or its customers are considering BYOD, knowing how to implement and deploy such a program helps to ensure the security of critical systems and data.
Company computers vs. BYOD

It’s hard enough for companies to secure their company-owned computers (servers, desktops, laptops, tablets and mobile phones), networks and devices (printers, PBX phone systems, etc.). It’s even more difficult for organizations to secure equipment they don’t own and control, especially when that equipment is used outside of the office where it can be lost or stolen and can reveal private information without proper security. When a company issues its own computers, its IT team can actively manage the ways in which they are used. For example, IT can implement security policies that ensure a computer’s operating system and software are patched (security flaws are fixed as soon as remedies for known security flaws are available), and anti-virus (AV) software is up-to-date. IT can also block users from visiting websites known for spreading malware and from downloading applications that have known vulnerabilities. However, companies can’t control what people do on their own devices. Many personal computers are infected, unbeknownst to users. If an employee connects his infected device to the company network, the device could infect the network and give hackers access to it.

Corporate-owned computers

If an employee uses a corporate-owned computer that only connects to the company network with a virtualized private network (VPN), the company-owned computers should be relatively secure, assuming the company follows best security practices. A VPN allows people outside of the office to work on the corporate network as if they were in the office. From any internet connection — public Wi-Fi or a home internet service provider (ISP) — the employee opens VPN software on their company computer and inputs security codes to connect to the corporate network. The employee is then securely tunneled in to the company network, allowing access to any files that are available at the office. Now, they surf the web as if they were inside the corporate network, protected by firewalls and other security controls the company has in place. It’s like being in the office, no matter where you are.

What are those security best practices?

- Employees are trained to never click on links or open attachments from unverified sources
- IT applies software patches as soon as they’re available and tested as secure
- IT has installed firewalls, intrusion detection and prevention systems, and AV software
- IT monitors the corporate network 24/7 for anomalies in incoming and outgoing traffic

But what happens when employees use their own devices to connect to the corporate network?
Concerns with implementing BYOD

When personal computers or devices connect to the company network, users bypass security systems that protect the network from outside threats. So if an employee connects to the corporate network on a personal device that has malware on it, that malware could migrate to the network. This is because network protections are typically configured to focus on preventing access from external computers and pay no attention to the traffic between computers already inside the network.

Protect the corporate network

Think of your network as a country with a system of roads, and the computers on the network are individual cities. Traffic from one city to another is monitored to some degree, but not closely controlled. Stronger security controls are in place at the borders of your country (your network). Border guards generally ensure that visitors with a legitimate interest in passing through your country are permitted to enter and the rest are turned away.

In a computer network, the border is guarded by a firewall. When someone outside of your organization connects to your website or corporate email, the request comes to your server wrapped in a package like an envelope. The firewall examines the package and looks at the internet protocol (IP) address of the sender. The firewall lets the package through as long as it is not from a blacklisted source known for being unsafe.

Also on the border is the intrusion detection system/intrusion protection system (IDS/IPS), which examines the contents of the package. If anything inside the package looks suspicious, the IPS blocks it. Once traffic has passed the border crossing, anti-virus software blocks known malware that may have gotten through the firewall and the IDS/IPS. But you cannot depend solely on AV software because it does not protect as well as the firewall.

When connecting to the company network through a VPN, a computer is given a free pass through all the border protections. Other computers on the network are still protected by their individual AV software but do not benefit from the broader border controls. With corporate-supplied computers, bypassing the border doesn't pose a significant additional risk because the connecting computer is maintained in a way that is consistent with the rest of its peers and is equally likely to be safe.

Threat actors are after money, sensitive customer and employee data, patent information, trade secrets and even access to your business partners.

BYOD, if not used securely, potentially opens one more window of opportunity for threat actors.
Personal devices

Personal devices are another story. Owners may not keep software up to date and may not have AV software installed. They may have visited websites that have infected links or downloaded applications that are infected with malware. In the absence of a fully patched environment and updated AV software, computers are easily infected, often within minutes of connecting to the internet. Once malware infects a user’s computer, it can spread to any device connected to that computer. If that device connects to the company network, that device’s malware can slide onto the network, bypassing all of the border security and ultimately allowing a hacker access to company servers.

As a precaution, organizations should never allow the following:

- A personal device (mobile phone, laptop, notebook or tablet) or USB flash drive to connect to a company computer or company network cable
- A personal computer to connect to the organization wireless network, but an exception can be made when that network is not connected to the corporate network
- A personal computer to connect to the company network through a VPN or any wireless channel

Remember that a VPN provides a private tunnel to the company network, so hackers cannot see traffic that flows from one computer to another. The VPN does not secure the network from malware. Some employees have surreptitiously downloaded software to their personal devices, giving them access to the company’s VPN. This should be prohibited.

BYOD can be safe if implemented correctly

Despite these cautions, BYOD can work safely. There are systems that can be put into place so that employees on personal computers can interact with corporate applications and data without being directly connected to the company network. Virtual desktop infrastructure (VDI) is one such system.

When a company deploys VDI, the personal device acts as the keyboard, monitor and mouse for a corporate-owned computer. The user runs applications and interacts with data stored on a company-controlled machine. The corporate server connects to the user’s computer only via the mouse, the keyboard and the screen, so the server cannot be infected.
Another type of system places a contained virtual bubble, like a software application, on each employee’s personal computer. When a user needs to work on a document or office application, they request the document or company application from the server. The server sends an instance, or copy, directly to the safe bubble where it is stored, so the user can work offline anywhere and make changes to the document. Because the bubble is contained in the computer, it is protected from any malware on the computer. The next time the user connects to the virtual system, the latest edition of the document is uploaded to the server. If a personal device is lost or stolen, or an employee leaves the firm, the contained bubble in their computer can be wiped remotely.

Before implementing any of these systems, it is wise to work with an independent security professional to review your needs, risks and budget to choose the type of system that suits you, preferably before your firm implements BYOD.

**Take a partner to implement a BYOD program**

It is usually impractical to manage your own BYOD program. Partnering with a mobile device management (MDM) vendor can help you deploy and support the use of mobile devices and corporate applications on mobile devices. Implementing an MDM solution can often be less costly than managing BYOD in-house, because MDM outsourcing companies have the knowledge and staff to work with countless types of old and new devices and operating systems. MDM vendors can manage multiple types of computer systems, password policy enforcement, remote device wiping, real-time monitoring and configuration settings. They can also address the major requirements of providing users with access to data and applications.

**Security Measures**

**Draft an employer-employee agreement**

In order to provide security for personal devices, organizations may need to have employees download software so they can be enrolled in the device management plan and can access corporate resources. Organizations supporting a BYOD program should have existing employees and new hires sign an acceptable use policy agreement that applies to the use of both corporate and personal computers.

The agreement should outline prohibited actions for BYOD participants. Participants should be prohibited from interfering with security controls placed on their personal devices or downloading any unauthorized software that gives them access to the company network. The agreement should also state what corrective actions will be taken should an employee attempt to circumvent the security controls. Additionally, the firm should provide a privacy policy that governs what the company can wipe remotely and what types of information, such as company email, it can access.
Security advice

There are many security rules, regulations and procedures your firm should follow to protect its clients and reputation. While a few appear below, an independent security consultant can best educate you on the risks and rewards of BYOD and help you develop the best solutions to fit your firm’s budget and needs.

- Provide employees with a list of devices your IT help desk can support
- Incorporate policies that require strong authentication and encryption solutions
- Educate employees so they understand the reasons behind the rules and policies

For more information, visit www.secureworks.com, email info@secureworks.com or phone 877.838.7947 to speak to a Dell SecureWorks Security Specialist.

Availability varies by country. © 2013 Dell Inc. All rights reserved.

Dell and the Dell logo, SecureWorks, Counter Threat Unit (CTU) are either registered trademarks or service marks, or other trademarks or service marks of Dell Inc. in the United States and in other countries. All other products and services mentioned are trademarks of their respective companies. This document is for illustration or marketing purposes only and is not intended to modify or supplement any Dell specifications or warranties relating to these products or services. July 2013