VOL. 6 | August 17, 2015

INFORMATION TECHNOLOGY UPDATE

BYOD: Balancing Risks and Benefits

The rise of consumer mobile computing devices such as tablets and smartphones has been accelerating at an astonishing rate. Most of us are attached to our mobile devices, and these devices have become a part of our lifestyle. Staying connected on a 24/7 basis has led to a number of challenges and opportunities for businesses looking to harness the power of these technologies to increase productivity, reduce costs, and increase employee job satisfaction. The Bring Your Own Device (BYOD) movement is an important consideration among companies looking to attract younger workers in a competitive hiring market. This article explores the BYOD risks and management strategies facing companies that have implemented or are considering BYOD programs for their employees.

A number of surveys over the past two years have examined the use and management of personal mobile devices in the workplace. While awareness and controls over these devices appear to be improving over time, adoption has been slower than originally projected, and there are still some concerns to report.

Approximately 40% of surveyed companies did not have any formal policies in place to govern the use of personal mobile devices and do not require employees to sign any form of security acknowledgement or agreement. Nearly one-third indicated they primarily rely upon end users to protect their devices and to remove data prior to trading their devices in. About a quarter of respondents admitted to having no implemented protections over sensitive company data on these devices. Studies have reported mixed results regarding increased employee satisfaction and productivity, and reduction in costs. In fact, some early adopters of BYOD have reported the exact opposite due to onerous policies, difficult-to-use technologies, and hidden costs.

Numerous risks associated with a BYOD program need to be considered before allowing personal mobile access to corporate information. The first step in developing a BYOD strategy is to conduct a thorough risk assessment. Following are some areas to consider when assessing BYOD risks:

- Reliance on end users to follow good security practices
- More headaches for IT if attempting to support these devices
- Unauthorized disclosure of corporate data through lost, stolen, or traded devices
- Increased risk of malware
- Information possibly being backed up to the cloud by end users
- Unauthorized access due to weak authentication controls
- Eavesdropping due to weak encryption controls
- Potential loss in productivity due to increased personal use on the job
- Lack of regular patching by end users
- Jailbroken or rooted devices that weaken security
- Possibility of additional social engineering attacks targeted at these devices
- Potential legal issues

2100 Corporate Drive, Suite 400 Wexford, PA 15090 | Phone (724) 934-0344 | Fax (724) 934-0345 | Email: info@srsnodgrass.com
1275 Glenlivet Drive, Suite 135 Allentown, PA 18106 | Phone (610) 530-8885 | Fax (610) 530-0409
2100 Renaissance Blvd., Suite 110 King of Prussia, PA 19406 | Phone (610) 278-9800

The FFIEC guidance on BYOD and mobile devices is limited, but guidance in other security areas applies to these devices. Certainly, organizations that allow BYOD need to have appropriate risk mitigation controls in place.

After completing a risk assessment, develop a corporate policy on mobile devices including personally owned devices that can be used to access corporate information. This includes defining the acceptable use of these devices, levels of support, liability and reimbursement rules, and disclaimers and security requirements, including monitoring and remote-wipe capabilities. Good communication and employee security awareness training are other key aspects of the program. When the company places control requirements over personally owed devices, there should be an agreement or security statement that is formally acknowledged by the employees who decide to use this technology. It is advisable to have legal counsel review these agreements prior to implementation. However, take care to develop a policy that provides the necessary protections without alienating potential users.

Security requirements are dependent on the types of access allowed, but generally the following areas should be considered within a BYOD program:

- In order to prevent unauthorized access, devices must be password protected using the features of the device. Also, strong passwords should be required to access the company network. Strong password standards should be adopted, including minimum length, age, history, and complexity requirements.
- Companies should consider multi-factor authentication methods such as soft tokens.
- The device should lock itself with a password or PIN if it is idle for specified period of time.
- After a specified number of failed login attempts, the device should be locked, requiring the user to contact IT to regain access.
- Rooted (Android) or jailbroken (iOS) devices should be forbidden from accessing the network.
- Require encryption levels that meet company standards.
- Address OS patching requirements.
- Require anti-malware controls.
- Register smartphones and tablets for corporate use. Smartphones and tablets that are not on the company's list of supported devices should not connect to the network.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- Enforce remote wiping of devices if the device is lost, the employee terminates his or her employment, or IT detects a data or policy breach, a virus, or similar threat to the security of the company's data and technology infrastructure.
- Monitor use and related security events with defined incident response procedures such as remote wiping of the device.
- Provide regular security awareness training.

Fortunately, companies don't have to build these capabilities from the ground up, as there are many viable vendor solutions available to help IT departments manage mobile devices. These range from solutions integrated into software suites as well as various point solutions. Consistent with the company's vendor management policy, there should be a thorough due diligence review of options available before selecting a vendor solution that best meets the need of the BYOD program. Once a vendor solution is selected, ongoing vendor assessments should be performed at least annually.

The risks associated with BYOD programs are significant but manageable with a diligent, thoughtful approach. To mitigate BYOD risk, it's necessary to focus on more than just the mobile computing device. A successful BYOD program needs to assess the potential impact on the entire network to protect confidential information. A holistic approach should be employed that includes sound risk management, governance including sound policies, layered security controls, continuous monitoring, and security awareness training.

Vendor solutions are available that can help companies implement the necessary security controls. The goal is to develop a program that is not too onerous for the employees or IT so job satisfaction and productivity gains can be realized while providing the needed protections. It takes some careful balancing to achieve.

Questions?

If you wish to discuss any of the above items, please contact Jeremy Burris or Rob Haller at (724) 934-0344, or email at jburris@srsnodgrass.com or rhaller@srsnodgrass.com.