The MEARIE Group

The Reciprocal

Insurance, Financial & Business Solutions June 2016

BYOD – Bring Your Own Device

According to Ernst & Young[1] by 2018 it is expected the number of mobile devices will be about 10 billion or **1½ devices for every man, women and child on the planet**. As these devices continue to proliferate, employees want the convenience of carrying one device, rather than carry a separate one for business. As such, companies are allowing employees to use their own devices for both personal and business purposes. **Welcome to BYOD** or Bring Your Own Device in the workplace. There are benefits for both the company and the individual when employees BYOD. Benefits include:

1. Increased satisfaction for the employees as they are more comfortable using their own device which they are familiar with, meaning a potential of increased productivity
2. Potential capital cost savings for the company for hardware, software, maintenance and licensing as individuals tend to replace equipment sooner

In addition to benefits, what risks does BYOD present to the company and to employees?

While there may be obvious benefits, there are also corresponding risks. Overall network security, keeping track of which devices may connect and security screening for personal devices interfacing with your corporate network may all be concerns. "BYOD significantly impacts the traditional security model of protecting the perimeter of the IT organization by blurring the definition of that perimeter, both in terms of physical location and in asset ownership."[2] While the potential savings or advantages may seem attractive, you must **consider all of the implications to exposing company data by allowing use of employee personal devices** which could have little or no controls. The policies and procedures you have in place related to your network and security can go a long way to mitigating potential risks.

Generally there are **three stages of implementing a BYOD program**[3] for your company:

1. Secure Mobile Devices

In order to develop a policy to ensure mobile devices are secure, it is important to understand the different types of devices, the different uses of devices and the territory in which devices operate. Once these elements are understood, a policy can be developed. **There are five basic areas that must be addressed in relation to securing mobile devices**:

- Lost and stolen devices – password protection, encryption, wipe data once device is lost.
- Physical access – due to the high number of lost or stolen devices, attackers have physical access to devices. It is harder to secure mobile devices once an attacker gains access.
- Role of user device ownership – BYOD makes it hard to separate business use from personal use. What about employee expectation of privacy to their personal information?
- Always on with increased data access – 24/7 access expands risk, as company data is always potentially exposed.
- Lack of awareness – user security awareness is a leading contributor of many risks and exposures.

[1, 2, 3] "Bring your own device - Security and risk considerations for your mobile device program." *Ernst & Young*. Sept. 2013. Web. June 2016.

See over…

2. Mobile Apps

From geography to social networking to productivity tools, "apps" have become a part of our daily lives. Controlling these various apps can present a problem for companies. Mobile Malware was cited as one of the top ten Cyberthreat Predictions for 2016.[2] RIMS indicated that security firm Veracode found a third of data breaches stem from attacks on apps, and RiskIQ reports that **17% of the top 150 apps contain malware**. The biggest problem is ensuring all updates and patches are applied in a consistent and timely fashion. One solution is to maintain an approved list of apps that can be used on equipment that will access your network and set standards for updates/maintenance installation.

3. Mobile Environment

With BYOD it is very difficult for a company to maintain control over device hardware, software and support. Each type of device will have varying models, OS and patches, all of which need to be kept up-to-date. Consider setting minimum OS standards for any device that will be connected to your network. Consider MDM (Mobile Device Management) software, to provide visibility, tracking and control of devices connected to your network.

If moving forward with a BYOD approach, **a corporate BYOD Policy is a must**. The policy needs to be flexible enough to meet individual user needs while protecting employee privacy expectations. It also needs to create security yet be manageable in addressing your company's security risks. The policy must be in-line with your other corporate policies relating to IT security, corporate governance, privacy and employment practices. The policy will need to be reviewed by your legal counsel. Users need to understand the policy and acknowledge they will abide by the policy to help protect your company security.

Whenever employee owned devices are connecting to your network, cyber security should be at the top of your corporate risk mind. **People are the weakest link in your defense against cyber risks**. Ongoing training and education are paramount and a constant reminder of the risks your company faces through all possible network connections. By developing, implementing and enforcing a well-developed BYOD Policy, you can begin to reduce your company's exposure to cyber risks from employees using their own devices at work. As with any company policy where potential privacy issues may arise, the final policy should be reviewed by your legal counsel for legal compliance, before implementation.

The following components should be included in your BYOD policy and reflect your operations:

1. Mobile device security requirements – anti-virus requirements
2. **Training – training and more knowledge regarding all cyber risks will equal less cyber exposure**
3. Password verification/authentication requirements
4. Encryption, storage and transmission requirements – use of cloud based applications
5. Automatically wipe device in event of loss or failed logon attempts
6. User restriction for mobile devices – i.e. no family or friends
7. Company liability
8. Company right to monitor, manage and wipe
9. IT support model and duties
10. Data usage while roaming or out of country
11. Acceptable use if different from normal use policy

Additional Resources:

- Clear Risk - What is BYOD, What Are the Risks, & How to Protect Your Business?
- Information and Privacy Commissioner Ontario
- 11 Best Practices for Mobile Device Management
- What is BYOD and why is it important?
- Computer Weekly: Business Must Be Clear On Data Privacy

This Reciprocal Newsletter is an electronic publication intended for Subscribers of The MEARIE Group's Insurance programs. It is published on a periodic basis and intended for information purposes only. In the event of specific claims, incidents or legal actions against the Subscriber, coverage will be determined by MEARIE policy interpretation.

[2] Tuttle, Hilary. "10 Cyberthreat Predictions for 2016." *Risk Management*. March 2016: 10-11. Print.