BYOD: UNTRAINED EMPLOYEES POSE A GREATER SECURITY RISK THAN HACKERS

Daragh Scaife outlines the benefits and the risks of Bring Your Own Devices.

Employees increasingly use their own technology to access work-related information held on corporate networks, a trend commonly referred to as Bring Your Own Device (BYOD). Indeed, around 65% of workers in 2012 considered their mobile device to be their 'most critical work device'. That's a huge leap from 13% in 2011.

BYOD is here to stay, due in large part to the advancements in mobile technologies and a more technology-savvy workforce. The white paper from Intuition *Implementing a Successful BYOD Programme* considers the benefits and risks associated with developing and implementing such an initiative from the perspective of training, cost and security.

TRAINING BENEFITS

- A powerful channel for an organisation to deliver effective learning, performance support, and general information to its workforce. Having access to content on a personal device ensures that learners can retrieve information at a time that is most convenient to them

- Employees who work non-traditional hours, and mobile workers who work remotely or travel frequently, find the use of personal devices liberating

- It empowers employees to learn because they can set their own pace, goals, and ultimately develop a sense of ownership over their progress – all key objectives for tapping into motivation

- On-boarding and training times are reduced because learning materials distributed via mobile devices are often more targeted, concise and engaging

COST BENEFITS

- Significant cost savings can accrue due to lower hardware and equipment costs, higher employee productivity and satisfaction

- Employees are quickly and easily able to access their organisation's corporate network

- IT department costs and workload are reduced as employees become responsible for maintaining their own devices

WHAT ABOUT SECURITY?

Allowing employees to access corporate networks via their own device can lead to data security concerns and increase the risk of data leakage. For example, the unintended exposure of confidential corporate data due to the loss or theft of a mobile raises the risk of damage to an organisation's reputation. It is therefore critical that mobile devices are protected from malware, phishing and other intrusive software related attacks.

The risk of hacking by cyber-criminals can also lead to damaging information leaks. Cyber-criminals are often highly skilled at manipulating target devices and operating systems with a view to installing malware and ultimately gaining either limited or full control of a device.

Malware, cyber-attacks and security breaches

If a cyber-criminal *is* able to gain control of a mobile device, they can perform a wide range of hacking activities – from intercepting calls and sending fraudulent message, to accessing confidential data, stealing financial records, and even remotely recording conversations. Some of the most common malware found on mobile devices are capable of the following:

- Generating persistent advertising pop ups
- Spying and/or tracking the device and its communications
- Stealing specific corporate information and sending it to third parties
- Unauthorised subscriptions to premium services
- Loss of control over the device; and continued downloading of other malware

The widespread adoption of mobile devices has predictably led to a significant increase in the number of cyber-attacks and security breaches in recent years. Between 2007 and 2012, there was a 35% increase in web application/server breaches and a 12% rise in email system breaches. Corporate information espionage is also growing at an alarming rate.

Worst of all, targeted cyber-attacks are being carried out quickly and effectively, meaning that most victims are unaware of what is happening until it is too late. However, organisations and employees *can* take the necessary steps and actions to protect their mobile devices based on the effective enforcement of a corporate information security policy. Here's how:

MOBILE DEVICE MANAGEMENT PLAN

The nature of a BYOD environment means that it is both open and complex. However, there *are* effective information security strategies and technologies that an organisation can implement in order to mitigate the security risks. One of the best ways to keep employees' technology secure is to develop a comprehensive Mobile Device Management (MDM) plan and information security strategy.

From an enterprise security perspective

Aside from the basic security measures on mobile devices such as a PIN number, code lock, auto lockout, encryption, and remote wipe features, there are additional security measures to consider when implementing a successful BYOD programme. Ideally, an MDM system will allow an organisation's network administrator to record and track all employees' activities on the corporate network.

If your organisation is considering a cloud-based MDM system, check to see if it provides access to log files that can provide a detailed history of which employees accessed what information; and when and where the information was accessed. You can take additional measures to minimise security risks by establishing a best practice 'Incident Response' plan. This defines detailed security procedures to implement when addressing security incidents such as the loss or theft of a device. This is what the plan should cover:

1. Assigning responsibility for the remote locking and/or deletion of data

2. Designating responsibility for the replacement of compromised devices

3. Defining the obligation and timeframe for the employee to notify the organisation of the accidental loss or theft of a device

4. Determining what will happen to corporate data stored, managed and used on the personal device of an employee who has left the organisation. Such policies may also include verification measures and checks to confirm that the deletion has been successfully completed

From an employee's security perspective

An organisation should address several key security considerations when implementing an MDM system. These include data back-up, data loss, loss of device, remote deletion, termination of employment, and convenience versus privacy. Here are some questions that need to be addressed:

1. Does the responsibility of the regular backing-up of data on devices fall to the employee or the organisation?

2. How often are data back-ups performed and who monitors compliance with such security procedures?

3. In the event of data loss, who will arrange for the recovery of information from the device; and who is responsible for covering the associated costs?

4. Are employees aware that during a data recovery process, personal and business data may be indistinguishable?

DEVISING A BYOD STRATEGY

Organisations need the ability to deploy across multiple devices and operating systems while maintaining efficiency, security and performance. The adoption of sophisticated tracking systems gives visibility and the ability to manage these factors. Currently, the most commonly used BYOD operating devices are Apple iOS (iPhone and iPads), Android, and WP7.

While the potential benefits of BYOD may outweigh the risks, an organisation should devise a strategy that incorporates educating employees about risks and benefits. It should take into account the challenges of managing and delivering content to myriad devices and platforms.

According to a recent survey, 72% of IT managers cite careless employees as a greater security threat than hackers. A lack of awareness about security policies may have the greatest impact to the security of mobile data. It is therefore essential that you provide regular and effective communications and security training to employees, to facilitate the successful implementation of BYOD. It is critical to identify the best way to harness the power of mobile technologies and to align investment in employee training with business performance.

A carefully planned BYOD implementation programme allows you to adapt and respond quickly to these challenges and opportunities. Robust policies and procedures include: comprehensive network security, management of employee devices, and the ability to deploy information across different mobile platforms. Such measures will ultimately save time and money, improve employee productivity and increase competitive advantage.

Sources

The Impact of Mobile Devices on Information Security – A Survey of IT Professionals:

http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report.pdf

Unisys survey conducted by International Data Corporation:

http://www.unisys.com/unisys/news/detail.jsp?print=true&id=1120000970016710190

The State of SME Security article on The Osterman Research survey:

http://www.smeadvisor.com/2012/10/the-state-of-sme-security/

Daragh Scaife is Head of Technology at Intuition.
www.intuition.com