Orion Investigations
20th Floor, Unit 2001-2002, 29 Sukhumvit 63, North Klong Tan
Wattana, Bangkok 10110

Orion Investigations

Computer Forensics | Mobile Phone Forensics| Malware Investigations | Training |Data Recovery

Computer Forensics Services

Turning to the Dark Side – The Dangers of Using Mobile Devices for Business

January 2014

Date: 13-01-2014

Author: Andrew Smith

Turning to the Dark Side – The Dangers of Using Mobile Devices for Business

With the introduction of the iPad in 2010, the tablet quickly emerged as one of the fastest selling devices in history. Tablets have achieved a level of adoption in 3 years that took smartphones nearly 10 years to achieve. In 2013, the adoption of smartphones in the US surged to 64 % according to the latest Nielsen survey.

Businesses have been quick to adopt mobile technology seeing the immediate benefits it has to offer. Employees are no longer tied to an office. They can maintain access to clients, emails, documents and the news while on the move. Customers have new ways to interact with a company and they are storing more data online. In terms of online retail time, mobile devices have now surpassed PC's. In June 2013 in the US, 55% of all online retail time was conducted on mobile devices.

Are businesses making full use of the mobile phenomenon? No not by a long way. The problem is that despite rapid growth, in many ways the mobile device market is still in its infancy. The majority of devices and applications or 'apps' as they are now known, are geared towards the consumers, not the business market. As the market matures the demand for business orientated apps will grow. Businesses will expect to be able to input data directly into their databases; generate and issue invoices and fully integrate their mobile devices into all aspects of the company network.

However, despite all the benefits those mobile devices have to offer there is a dark side. Businesses have been quick to make use of mobile technology with very little thought to the security implications.

Many businesses are providing their employees with mobile devices or allowing employees to connect BYOD's (Bring Your Own Device) to the network. The trend for mobile devices is for data to be backed up to one or more online storage locations. As a result, with BYOD's the line between the storage of personal data and business data is now blurring. The business has no control over where the data is stored online or any idea of how secure the online storage actually is. Allowing mobile devices to be connected to a network without the proper security systems in place means businesses have lost control of one of their most valuable assets, their confidential data. They no longer have control over who has access to that data.

Symantec recently released the 2013 Norton Report. Below are just some of the worrying statistics that they have identified:

- 57 % of Smartphone/tablet users are not aware that security solutions for mobile devices exist.
- Nearly 50 % of users do not use basic precautions such as passwords, security software or back up their files from the mobile device.
- 38 % of users experienced mobile cybercrime last year.
- 27 % of adults have lost their mobile device or had it stolen in the last 12 months.
- 49 % of users use their personal device for work and play.
- 20 % of users share work related information with friends and family.

Even when steps have been taken to secure the mobile device, this is no guarantee that the data will remain secure. Many users have fallen victim to unscrupulous mobile phone repair shops that have made copies of private data which has then been posted to the Internet, as seen in a recent BBC article. To avoid this type of problem it is vital that all data is removed from the device before handing it in for repairs.

Another, often ignored, aspect of mobile devices is the issue of malicious software (malware). Malware authors are now targeting mobile devices by creating malicious apps designed to steal data from the device. According to Trend Micro there are now over one million Android-based questionable and malicious applications in the wild. If you think you are immune by using an IOS device, think again, malware authors are also beginning to target IOS devices. Many of the malicious apps are known as premium service abusers, which sends unauthorized text messages to certain numbers and register users to costly services. Malware authors are also now targeting mobile users' banking transactions by creating apps that are capable of intercepting the One Time Password (OTP) SMS message.

Allowing unsecured devices to be connected to the company network increases the risk of the organization being a victim of employee fraud.

Below are just some of the highlights from the Symantec report "What's Yours Is Mine: How Employees are Putting Your Intellectual Property at Risk".

- 50 percent of employees who left or lost their jobs in the last year have kept confidential corporate data, and 40 percent of them admitted to planning to use that content in their new jobs.
- 56 percent of employees don't believe it is a crime to use a competitor's trade secret information.
- 62 percent of employees thought it was acceptable to transfer work documents to personal computers, tablets, smartphones or online file sharing applications.

Let's take a moment to look at the stages an employee will typically go through before committing a fraud.

What is important to remember is that fraud is not a random occurrence. Fraud will occur when the conditions are right. Most employees do not set out to defraud their employer but the fact is the majority of people have the potential to become a fraudster under the right conditions. The three conditions are motive, opportunity and rationalisation. This is often referred to as the Fraud Triangle. In order to prevent fraud you need to remove at least one of the three conditions.

Motive – is a need or pressure felt by the person committing the fraud. Maybe they are under financial pressure from medical bills, they need to support a family or have gambling debts. It could be pressure

from work to meet targets, get that promotion or bonus. It could also be from a strong desire to own the latest material goods such as cars and houses which are beyond their normal means.

Opportunity – the opportunity arises when a person has access to information and assets and there are no suitable processes, checks or balances in place to monitor what is taking place. Employees often have access to information beyond what is needed for them to perform their role. Opportunity is the one condition that employers have the greatest control over. Without the proper safeguards in place it will only be a matter of time before fraud will occur.

Rationalisation – is the one thing we are all good at and do on a daily basis without even realising it. When we are driving and we exceed the speed limit we rationalise that it is ok because we are only just over the speed limit, the roads are empty or we need to arrive on time. Within the work place employees rationalise that it is ok to steal from the company because nobody is getting hurt, the company doesn't appreciate the good work that has been done, are unfair on their employees or that they will never miss the money or assets. This is the hardest condition for an employer to deal with.

When an employee chooses to leave a company or their employment is terminated, the company is faced with the issue of how to ensure all of the company data has been removed from BYOD's and from online storage locations. We can see from the above information that without the proper safe guards in place the employee who has the motivation, has the perfect opportunity to misuse the data.

Although there is significant risk with BYOD's and a case of balancing risk versus privacy, all is not lost. Many companies who have successfully and securely integrated BYOD's into their networks have done so by working closely with their employees to understand how they use their devices and to allay their fears about breach of privacy. As a result they have successfully introduced policies that comply with privacy laws while keeping company data secure. Mobile device management (MDM) vendors now provide solutions for dealing with BYOD's. Many of the applications offer what is referred to as a 'sandbox' approach where the company has control of the corporate data but are unable to see or access any of the employee's personal data. Selective wiping has now become the norm. When a mobile device is lost, only the company data, settings and apps are wiped while leaving the employee's personal data intact.

As the functionality and performance of mobile devices increases, incorporating them into the company's network will bring enormous benefits to both the employee and the company. With careful planning, the

introduction of carefully thought out policies and the right security software, the risks that come with mobile devices can be drastically reduced for relatively little cost.

About the Author

Andrew Smith – Director of Computer Forensic Services, Orion Investigations

Andrew is responsible for the management of the Orion Computer forensic Unit. His responsibilities include ensuring the unit operates to the highest international standards, business development and the development and delivery of training for clients and staff. Andrew is an experienced forensic investigator with extensive training and comprehensive experience in relation to criminal, corporate, malware and counter terrorism investigations within the UK and Europe. He has worked in the public sector with the South Yorkshire Police where he received his initial training in computer forensics and also in the private sector with a leading UK computer forensics company. He is also an experienced trainer having developed UK Law Society approved training courses and delivered master degree level forensic training. With over 11 years' experience in the field of computer forensics Andrew has regularly appeared in court as an expert witness to present complex computer evidence.