

Mobile Computing: Rise of the Machines!!



An ambiguous reference to an Arnold Schwarzenegger movie may seem an unusual place to begin a white paper on mobile computing, however, given that globally there are approximately three hundred and seventy million smartphones and thirty million iPads in use on a daily basis, not to mention two billion internet users, it just goes to prove that fact can be stranger than fiction. Many of the threats sound like they pose a serious risk to humanity; including botnets, trojans, zombies and perhaps slightly less intimidating, but by no means less daunting, phishing.

The security of connected mobile devices in the workplace should be a prominent consideration for an organisation's security strategy because data breaches involving lost or stolen laptop computers or other mobile data-bearing devices remain a consistent and expensive threat. It's the increasing sophistication and convenience of mobile devices such as laptops, smartphones, tablets and USB sticks that contribute to both their popularity in the workplace and their risk to an organisation's networks, data and reputation. Research suggests that mobile device-related breaches have consistently cost more than any other types of data breaches.

What are mobile devices?



"Mobile devices" can mean many different things to different people. Examples include:

- Full-featured mobile phones with personal computer-like functionality, or "smartphones".
- Laptops and netbooks.
- Tablet computers including iPads, Playbooks etc.
- Personal Digital Assistants (PDAs).
- Portable Universal Serial Bus (USB) devices for storage (eg "thumb drives" and MP3 devices) and for connectivity (eg Wi-Fi, Bluetooth and HSDPA/UMTS/EDGE/GPRS modem cards).
- Digital cameras.
- Radio frequency identification (RFID) and mobile RFID (M-RFID) devices for data storage, identification and asset management.
- Infrared-enabled (IrDA) devices such as printers and smart cards.

What should you do?

Many organisations start with the devices themselves, and focus on how they, and the infrastructure they reside on, can be secured. Whilst this is extremely important, the real threat is posed by the data that is stored/accessed by these devices. To this extent, organisations should ask themselves, "Do I really understand my data estate?"

The reality is that very few organisations truly understand the extent and nature of the data they hold and how this

flows throughout their business. To achieve an accurate picture, you will need:

Data permeation maps

These document the flow of data from inception through to destruction; they incorporate where the data resides – this could be across multiple locations, platforms and applications; whether or not it leaves your environment or is shared with a third party; the controls that reside over the data; the respective legal and regulatory requirements; and the data classification e.g. Confidential, Business Use Only, Public etc.

Enterprise strategy

In parallel with this, you need to develop an enterprise strategy for mobile security. Mobile devices create new challenges for IT and security practitioners, which demand a holistic or strategic approach to managing risks, threats and vulnerabilities without diminishing user convenience or productivity. The solution is to accept the fact that mobile devices are now a way of life and not over-limit the use of these devices.

In order to create an enterprise strategy it's recommended that you conduct an audit to determine where mobile devices are used within the organisation. An audit helps to determine the technologies that limit access to, or transfer of, sensitive and confidential information, and associated risks.

Mobile policy

Create a comprehensive policy (including detailed guidelines) for all employees and contractors who use mobile devices in the workplace. The policy should address the risks associated with each device and the security procedures that should be followed. You should also establish rigorous monitoring practices and implement enabling technologies to ensure policies and guidelines are strictly enforced. It's important to validate that policies are being followed and employees are in compliance. Therefore, mechanisms should be in place to detect non-compliance and deal with negligent or malicious employees.

Organisational accountability

Establish organisational accountability. Organisations have a responsibility to provide their employees with the policies, procedures and technologies necessary for the security of mobile devices used in the workplace. In turn, employees must be aware of their need to be accountable and aware of the importance of using their mobile devices responsibly. Understand that it is almost impossible to keep employees from using mobile devices for both

personal and business purposes. Therefore, create guidelines for the responsible use of these devices when used for non-business purposes.

Employees should be instructed to be vigilant to prevent malicious software on their phones. They should be advised to be wary of texts, system messages or events on their phone that they did not ask for, initiate or expect. They should turn off Bluetooth if they are not using it. Use encryption software that works worldwide to secure sensitive calls and stored data.

Application controls

Apply application controls, patching and other controls to prevent hacking and surreptitious malware infections. With so many targeted attacks exploiting vulnerabilities, it is vital that the operating systems and applications on mobile devices such as browsers, pdf readers and flash players have current patches applied. Application control can ensure that only patched, secure applications are used for internet access. On company-owned smartphones, policies to block unproductive or risky applications should be enforced. In addition, you should also restrict use of Exchange Active Sync or other email synchronisation to user-owned devices that comply with your security policies such as minimum password length.

Whenever feasible, use remote wipe, mobile device encryption and anti-theft technologies to reduce data breach risk. In addition to encryption, the organisation should seriously consider anti-theft technologies that can be used to locate a lost device or prevent unauthorised parties from re-using a device. Most smartphones have remote wipe capabilities that should be enabled so that you can wipe the data on a lost device. You may need to invest in software to manage this capability. To avoid needing to disclose a lost device as a potential data loss, you will need to have a central reporting system that can demonstrate that a lost device was either encrypted or remote wiped.

Emerging privacy issues

Understand emerging privacy issues inherent with mobile devices. The exposure of customer or employee personal information can result in reputation damage and costly fines as a result of non-compliance with legislation. Conduct privacy impact assessments that closely examine the privacy and data protection risks associated with mobile devices.

Outsourcing data to third parties creates another level of data protection and privacy risk for the organisation. It is important that third parties have the capability to

safeguard customer, consumer, or employee data at the same level of integrity that exists in-house.

Threats on the move



Device makers and wireless service providers have long focused on communications and other services, with security remaining an afterthought. Security is now playing catch-up with the rapid adoption of Android and other smartphones, all of which are hard for organisations to manage. The

number and types of mobile threats—including viruses, spyware, malicious downloadable applications, phishing, and spam—have spiked in recent months. For instance, McAfee Labs' threat report for 2010's fourth quarter reported a 46 percent increase in malware targeting mobile phones over the same time period the previous year. This equated to more than 55,000 new pieces of [mobile] malware on a daily basis.

Mobile communications can use the same types of security, including antivirus and firewall products—as fixed communications. This lets businesses enforce security policies about which users and devices can access specific corporate applications.

Devices are likely to face a growing number of the types of attacks traditionally launched against desktop systems. This will place increasing importance on mobile device makers having organisational security features and configuration options in place. It will become necessary for security to be considered in all phases of application development to ensure that resilience against attacks is built into mobile devices from the start.

So what should I be worried about?

Botnets

Attackers form a botnet by infecting multiple machines with malware that victims generally acquire via e-mail attachments or from compromised applications or websites. The malware gives hackers remote control of the “zombie” devices, which can then be instructed to perform harmful acts in concert.



Malicious applications

In some cases, hackers have uploaded malicious programs or games to third-party smartphone application marketplaces, such as those for Apple's iPhone and Google's Android devices, or have otherwise made them available on the internet. These malicious apps are usually free and gain access to a phone courtesy of users voluntarily installing them.

Social networking

As smartphone use has grown, so has mobile social networking. Malicious links on social networks can effectively spread malware. Participants tend to trust such networks and are thus willing to click on links that are on “friends” social networking sites, even though (unknown to the victim) a hacker may have placed them there.

Spyware

Hackers can use spyware available online to hijack a phone, allowing them to hear calls, see text messages and e-mails, and even track a user's location through GPS updates.



Bluetooth

Bluetooth enables direct communication, including the sharing of content, between mobile devices. Wireless devices can broadcast their presence and allow unsolicited connections and even the transmission of executables if users don't configure their Bluetooth operations appropriately. These are files in a format that the computer can directly execute. Unlike source files, executable files cannot be read by humans..

Wi-Fi

Hackers can intercept communications between smartphones and Wi-Fi hotspots. The fundamental vulnerability is hotspot architecture with no encryption to protect transmitted data.

Phishing

Phishing is an attempt to gain access to sensitive information by pretending to be a trustworthy entity and poses the same risk on smartphones as it does on desktop platforms. In fact, many users trust their mobile device more than their computers and thus are more vulnerable to phishing.

Conclusion

Mobile devices are emerging as one of the most serious threats in organisations. They have the potential to become the biggest threat for leakage of confidential information. Their protection, very much neglected until recently, will become a primary task for organisations. They are changing the business landscape. As organisations have moved toward global business operations, these devices have become indispensable.

Many of the risks associated with mobile devices exist because of their biggest benefit which is portability. Mobile devices frequently transport data via wireless networks, which are typically less secure than wired networks. These wireless networks can leave information at risk of interception. Additionally, many of these devices have storage capability and unencrypted data "at rest", thus the information gathered from either the interception of data in transit or theft or loss of a device can result in the compromise of sensitive and proprietary information.

While many organisations have chosen to utilise this technology, often they have not considered the business risk or the governance implications associated with these devices. Loss, theft or corruption of sensitive or confidential data; malware that can affect not only the mobile device itself, but also the enterprise network; and the way in which employees use the devices are just a few of the risks involved with this type of technology.

Once the risks and benefits of mobile computing are understood, businesses should implement a governance

framework to ensure that process and policy changes are implemented and understood, and that appropriate levels of security are applied to prevent data loss. Creating a transparent, understandable, flexible and executable policy to protect against risks related to the use of mobile devices will support management in its effort to protect intellectual property and sustain competitive advantage.

Can we help?

Kingston Smith Consulting operate an experienced model and all our consultants have a minimum of 10 years experience working in their chosen sector and each combines experience in a line role in industry with their career as a consultant.

Our Technology Risk Management professionals approach each engagement with a "can-do" perspective gained from years of working in high-risk, high-stakes IT environments.

We are able to provide a range of solutions to protect your business.

If you have further queries, please do not hesitate to contact Mark Child for more information.

Tel: +44 (0)20 7566 3731

Fax: +44 (0)20 7689 2475

Mobile: +44 (0)7515 107005

Email: mchild@kscllp.co.uk

About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice of the top 20 accountancy firm Kingston Smith LLP.

Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in over 50 countries around the world.

Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010
info@kscllp.co.uk www.kscllp.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD