Mobile Devices and Organizational Security Risk

The Prevalence and Power of Mobile Devices
Mobile devices are ubiquitous—almost everyone has one (or more). Mobile device usage is steadily growing as the technology in mobile devices becomes increasingly more powerful and universal. Mobile phones are continually adding storage capacity, processing power, battery lifetime, and display abilities while consistently reducing the size of the devices. The functionality of disparate technologies such as MP3 players, GPS navigation, PDA, cameras, and game systems are being integrated into mobile phones, dubbed “smart phones.”

A fairly recent phenomenon for mobile devices is the advent of app stores. App stores provide a single location to download or purchase a multitude of applications that can provide amazing functionality that is not present on the device when it is shipped from the manufacturer. Although mobile devices have had the ability to run third-party applications for some time, these applications were typically limited to simple games or extremely basic business functionality not synched with internal business environments. Mobile applications are not basic anymore. The functionality of mobile applications now ranges from augmented reality to video conferencing to complete office software to custom applications used to access internal business systems via the Internet.

Utilizing third-party applications from app stores, smart phones are increasingly capable of providing much of the same basic functionality of a conventional laptop with additional unique advantages that are not possible in other computing devices. Mobile devices are almost always with the employee, always turned on, and always have a data signal. This leads to anytime access to anything, and, as result, is causing an increasing number of people to rely on their mobile device as a mini-computer while traveling or away from the office.

Anytime access to corporate email, databases, files, documents, internal business applications, etc. is great for employee productivity, but it presents security risks.

Mobile Security: A Top Concern
During the time that mobile usage has increased, organizations have been investing large amounts of capital and time to develop and implement information security policies, procedures and practices to mitigate their risk exposure in traditional computing assets such as servers, desktops, routers, laptops, etc. Although the advantages that mobile devices provide are fairly obvious, there are a large number of risks associated with the use and reliance on mobile devices that must be considered. The increase of mobile applications and device storage makes it possible for an employee to literally “carry” larger, more complex and more sensitive data in their pocket.
The security market for products and services to address traditional computing assets has reached a level of maturity that dwarfs the infancy of the mobile security market. The risk profile of mobile devices closely resembles that of traditional computing assets. Despite having similar risk profiles, mobile devices do not currently have a matching profile of mitigating technologies. Traditional computing devices are typically managed by the enterprise. Enterprise management provides assurances that devices have approved operating systems and software, receive security updates, have virus/malware/spyware protection, maintain proper asset management and use encryption where appropriate. Mobile devices are often not managed by the enterprise; therefore, there is no assurance that the devices satisfy corporate security policies.

In addition to the lack of enterprise management, there are currently a limited number of mobile solutions available to satisfy corporate security policies. The solutions that exist are limited in their usefulness due to the multitude of operating systems in use throughout the mobile device industry. Multiple communication mechanisms such as Bluetooth, Wi-Fi, USB, infrared, and removable media must be considered, creating more channels to secure.

There are also significant risk factors that are either unique or significantly increased in respect to mobile devices. Since mobile devices are, by design, small and ultraportable, physical access is easy, physical security is almost non-existent, and the risk of losing a mobile device is significantly increased when compared to traditional computing devices. Another noteworthy threat is that a mobile device will come into the hands of an unauthorized user via device turnover. Since these assets are typically not owned or controlled by the enterprise, the employee is able to sell, give away, trade-in or simply throw away the existing device when it is replaced and who’s keeping track of what corporate information might be on that device?

**Consumerization: A Key Issue**

Organizations must also deal with the consumerization of mobile applications and devices, which can cause problems for IT departments. Employees want to do the same things on their work devices that they do on their personal devices, so they are pressuring their employers to let them do so. Or, employees have found ways, often unapproved, to access corporate data on their personal devices. The employees are essentially running the show. In addition, many organizations now allow employees to pick their own mobile devices, enabling them to take advantage of the newest technology. However, all of these things can lead to challenges with maintaining adequate security.

Attempting to ban cool new mobile devices is a losing battle. IT is no longer in a position to inhibit technology that improves business productivity. These devices are now just too ubiquitous and too indispensable. Instead of finding ways to stop smart phones from accessing Salesforce.com, IT needs to be thinking about how to extract higher value out of knowledge workers.

CXOs have to figure out how to authorize the right level of mobile functionality, while at the same time controlling risk.

**A Multitude of Attack Vectors**

Smart phones have a large surface of potential entry points for a compromise. Although “traditional” computers and laptops possess many of the same technologies as modern mobile devices, many are not nearly as viable as they are in mobile devices. Short-range communication protocols such as Bluetooth, Infra-red and Wi-fi are more viable avenues of exploit (although still not ideal) due to the ultra portability of modern mobile devices.

The list below categorizes some of the potential attack vectors for mobile devices:

- SMS
- Wi-fi
- Bluetooth
- Infra-red
- USB
- Web browser
- Email client
- Third party applications
- “Jail-broken” phones
- Operating system vulnerabilities
- Physical access
Potential Information for Compromise
A compromised mobile device can provide a wealth of information to an attacker. The following are examples of possible targets for attackers:

Communications
- **SMS**
  - SMS messages on the device can be forwarded to the attacker, or the attacker can search them for valuable information.
  - Many commerce sites, including financial institutions, communicate one time passwords or credential information through SMS as an out of band channel.
  - SMS can be utilized as a means to perform transactions that can lead to an attacker performing unauthorized transactions from the device.
- **Email**
  - If the device is being used to send or retrieve email messages, the messages can be forwarded or searched by an attacker. This includes private as well as corporate email messages.
  - Email messages could likely contain sensitive company information as well as potential other private information such as credentials from password reset links.
- **Phone**
  - Low-level access to the hardware of mobile devices through mobile operating systems can provide an attacker the ability to record or listen to voice conversations.
- **Video/Photo**
  - Low-level access to the hardware of mobile devices through mobile operating systems can provide an attacker the ability to activate the internal camera to record video or take photos from the phone to provide detailed views of the device’s surroundings.
- **Social Networking**
  - Social networking applications running on a smart phone can be utilized to propagate malware through the trust of the users associated with the compromised account.
  - Impersonating as the associated account can allow the retrieval of personal information about the user and their social contacts.

Location Information
- Most new mobile phones provide location information (for example, using built-in GPS or GSM antenna info) so it may be possible for an attacker to query this information on the device to determine where the device is located.

Voice Recording
- Low-level access to the hardware of mobile devices through mobile operating systems can provide an attacker the ability to activate the internal microphone to record any sound or voice close to the mobile phone. This, of course, includes phone calls.

Documents
- The attacker can retrieve documents stored on the device, including attachments from emails.
- Document types can include PDF files, Microsoft® Office files, credentials, encryption certificates, internal videos or internal e-books, among others.

Credentials
- Cached credentials may be stored insecurely inside third-party applications.
Mobile Devices and Organizational Security Risk

**Previous Security Issues**
The following security issues demonstrate various threat scenarios on mobile devices. This list is not meant as an all-inclusive list of potential threats, but it is meant to demonstrate some known threats.

**Terdial.a**
Terdial.a is a Trojan that makes expensive background phone calls to an international number. The Trojan was placed inside of a game called “3D Anti-terrorist Action” and uploaded to common Microsoft Windows Mobile download sites.

**Malicious Android software**
In December 2009, a user named Droid09 uploaded multiple mobile banking applications to the Google Android Market in an attempt to steal financial credentials of unexpected users. The applications were discovered to be fraudulent and subsequently removed, but some credentials were obtained prior to the removal of the applications.

**Malware**
There are commercial applications available for most mobile devices that provide full spying capabilities. Most are marketed as applications to ensure the safety of children or track cheating spouses. These applications can capture voice calls, SMS messages, email messages, web traffic, account credentials and just about anything else that you can do on a mobile phone. These applications demonstrate the capabilities of malware and will likely be utilized in future attacks.

**BBProxy BlackBerry Tunnel**
A security researcher developed a piece of software for use on BlackBerry devices. BBProxy allowed an attacker to use the BlackBerry to tunnel inside the user’s corporate network.

**BlackBerry PhoneSnoop**
PhoneSnoop is a malicious mobile application released in October 2009. With this program installed on a BlackBerry device an attacker is able to monitor any incoming or outgoing calls that the phone makes.

**BlackBerry SS8 Interceptor**
The United Arab Emirates mobile provider Etisalat distributed a 2009 BlackBerry software update that included surveillance software. Once installed, the software forwarded all email to the provider and law enforcement.

**“Curse of Silence” Worm**
The “Curse of Silence” exploit against several current versions of Symbian S60 phones was demonstrated at the end of December, 2008. The exploit was very easy to utilize and a video demonstrating how to perform it was quickly distributed on the Web. The resulting effect of the exploit jams the victim’s SMS messaging. Many network operators reacted quickly and started filtering their SMS traffic so as to prohibit the exploit message. Nokia later released a free recovery utility called “SMS Cleaner”. The exploit was, at best, a potential nuisance with little profit motive, and has not been widely reported to have been used.

**iPhone PDF Font Rendering Exploit**
Mobile Safari in v4.0.1 of Apple’s iOS firmware is vulnerable to a remote web based attack that can completely bypass the security sandbox used by iOS. The exploit has been set up to jailbreak iOS devices running v4.0.1 and lower. The jailbreak allows users to install unauthorized software and access low-level hardware functionality on the devices. Although the vulnerability is being cited as an easy method to jailbreak an iOS device, the security ramifications of the complete bypass of the firmware sandbox simply by viewing a PDF file have not be widely discussed.
Jailbroken iPhone Worms
All of the following Apple iPhone worms exploit Jailbroken iPhones with SSH installed using the default root password of “Alpine”.

- **Ikee Worm**: This worm changes the background of the iPhone to famous popstar Rick Astley (a.k.a. a RickRoll).
- **Ihacked**: This worm changes the background of the iPhone to a screen asking for money to get rid of it.
- **iBotnet.A**: The iBotnet.A was used to steal account information from customers of ING Direct.

Symbian/Windows Trojan
There are a number of Trojans that affect Symbian based mobile phones. There is a growing number of Trojans that also place Microsoft Windows® software infected with a trojan onto the memory cards that can infect a Windows PC when the memory card is used on a Windows machine.

- **Cardtrap**: There are several variants of this Trojan. They disable several built-in Symbian applications and attempt to damage several other third-party applications. Several variants place Windows software infected with malware onto the memory cards of the infected devices.

Authentication Bypass:

- **iPhone Access to Private Data**: iOS 2.0.2 (formerly iPhoneOS) and earlier allowed a malicious user with physical access to an iPhone to bypass the PIN lock and access contact information, web pages, email messages, and SMS messages by utilizing the emergency dialing capabilities of the iPhone.
- **iPhone Access to Private Data (2)**: The iPhone 3GS was advertised to have file system encryption of private information stored on the device. The encryption is not based on a PIN, passphrase or key, making it easy to retrieve the information from the device without the user's valid PIN.
- **webOS SMS Injection**: Palm webOS is a mobile phone operating system that is designed as a web browser and utilizes standard HTML and Javascript for its applications. Since applications are written using HTML and Javascript, they are susceptible to standard web exploits. An injection vulnerability was discovered that allows an SMS message to execute programs on the mobile device without interaction from the user.

Possible Future Attack Vectors
In the future, credit card payment processing and bar code scanning, such as electronic boarding passes, would be likely targets.

Regulatory Compliance Requirements Must be Addressed
Information security compliance isn't simply developing security policies and satisfying assessments and audits. It's about having a deep understanding of risk and how to manage it, in order to best utilize opportunities. Failure to establish an effective security compliance program can have serious consequences, including fines for non-compliance and greater regulatory oversight.

Healthcare is an example of an industry that may increasingly benefit from the use of mobile devices to monitor and treat patients, both in health facilities and at their homes. But if security is outdated or ineffective, the damage can be costly from a non-compliance perspective. For example, a civil penalty from the Department of Health and Human Services for a HIPAA data breach violation can now be as high as $1.5 million. That figure does not even take into account the cost of lost data and lost revenue due to tarnished reputation.

Another highly-regulated industry that will become increasingly affected by mobile security issues is financial services. The use of mobile payments or mobile banking can be risky, especially when users connect to unsecured WiFi hotspots. As the financial industry rolls out more mobile banking options to consumers, the risks could become more widespread.

It’s become clear that a thorough mobile security risk assessment and mobile security strategy is essential to meeting and maintaining compliance with various industry information security requirements.
Inconsistent Security Updates

Until recently, mobile devices were not designed with a mechanism to receive operating system or application updates. There still is not a consistent method to provide updates, but some manufacturers, carriers and developers are beginning to recognize the need to provide users with security updates. The lack of a consistent update process for mobile devices hampers the ability of users to verify that their device contains all pertinent security updates.

Addressing Mobile Security Can’t Wait

Corporations must use diligence and begin addressing the security concerns of mobile devices, now. Attention to security while a technology is developing is the key to ensuring that the technology grows into a reliable and trusted tool that can be used by the ever-increasing mobile workforce.

The U.S. Department of Commerce recommends the following in their Guidelines on Cell Phone and PDA Security:

- Organizations should plan and address the security aspects of organization-issued cell phones and PDAs.
- Organizations should employ appropriate security management practices and controls over handheld devices.
- Organizations should ensure that handheld devices are deployed, configured, and managed to meet the organizations’ security requirements and objectives.
- Organizations should ensure an ongoing process of maintaining the security of handheld devices throughout the lifecycle of the device:
  - Requesting the device
  - Purchasing the device
  - Ongoing use
  - Disposal of the device

Organizational Benefits of Effective Mobile Security

When an organization effectively secures their mobile environment, it contributes to better security for the entire enterprise. Devices with inadequate security can lead to data breaches of sensitive corporate information through physical loss, malware, Trojans, worms, and spyware. Mobile misuse related to SMS, data, and voice is also a cost and security issue. Effective security helps control costs by proactively securing applications before malicious intent, not after its effects.

Appropriate mobile security helps enterprises address the information security requirements in regulatory mandates and contracts. Loss or theft of data could expose the enterprise to risk of non-compliance with various identity theft and privacy laws. The right security helps mitigate the effects of fraud or compromise, therefore protecting an organization’s brand and reputation.

In addition, successful mobile security enables broad mobile use within the corporation, versus limiting usage and associated productivity. Employees can do more and access more from their mobile devices, such as ERP and CRM applications, or Salesforce.com. The CXO is in the position to say “yes” to the next business-enabling mobile technology access request when mobile security is properly addressed within the organization.

Steps to Addressing Mobile Security

Organizations should consider the following questions when determining their needs for mobile security:

- Do you have any mobile applications that your customers/partners access?
- Does your organization have any data on mobile devices that is worth protecting?
- Does your organization need to comply with any regulation that governs loss of specific types of data?
- How do you know if your mobile applications have been developed and deployed securely?
- Do you utilize third parties in the development of your mobile applications?
Most organizations will find that they do indeed have a need for mobile security, and could use guidance on the most effective best practices. These include:

- Force encryption of data at rest on mobile devices
- Force secure connectivity on unsecured public networks
- Confirm unauthorized mobile devices do not have access to corporate LAN
- Confirm mobile user spending is in line with the mobile policy and additional costs can be recovered
- Over-the-air decommissioning (remote bricking) of lost or stolen devices to help prevent access to the data
- Authentication: set the device to auto-lock; set limit for unauthorized login attempts
- Keep device out of sight when not worn
- Handheld devices should be enterprise property
- Before an employee departs, obtain device and remove corporate data
- Have a clear policy on remote data deletion and do not hesitate to execute it
- Classify data according to the sensitivity of the data carried
- Only permit digitally signed applications
- Be agile—quickly and flexibly adapt to changing mobile landscape

Choosing a Qualified, Experienced Mobile Security Provider

Most organizations will find that they could use help in addressing the complexities of mobile device and application security. As mobile device processing power is increasing, more sophisticated security controls can also be applied, and it's important to work with a provider who has a comprehensive understanding of all of the issues. A qualified provider should have expertise across three key dimensions—business, operations, and technology—because they combine to control the costs, and strengthen the security of the device, information and your overall organization. The provider should offer solutions that leverage existing assets, personnel, and technologies, and should provide coverage across the entire project lifecycle, including consulting services and managed security services.

In order to help organizations secure their mobile applications and the underlying supporting infrastructure, a provider should have wide and deep experience with all aspects of security. For example, they need to understand that applications function more like native apps rather than utilizing a standard browser and that mobile apps are not restricted to using standard HTTP/HTTPS. They must also have access to many security testing resources, as fragmentation in hardware, operating systems, applications, and operators can present challenges. For example, there are multiple versions of the same applications for disparate mobile operating systems. In addition, there are countless mobile devices, and the supported technologies (communication, access control, storage, etc.) vary by manufacturer and OS (Symbian, Oracle J2ME, Qualcomm BREW, iPhone, Windows Mobile, Window Phone 7, webOS, and Android). Lastly, the provider must have expertise with convergence across multiple dimensions: voice and data; fixed and mobile (Wi-Fi and cellular); and PC and phone, because all are interrelated when it comes to successful mobile security.

The provider should be able to provide access to expert resources internally and externally, and transfer effective best practices that have been proven to work. A reputable provider serves the decision support role, guiding an organization to make the right decision, regardless of whether the solutions leads to them, a partner, or the customer organization internally.

Conclusion

When an organization enhances their mobile security, as well as their overall information and infrastructure security, they are doing the right thing to protect their employees, their intellectual property, their money, and their reputation. Working with a knowledgeable, experienced provider can make a difference in establishing a comprehensive mobile security strategy, and more importantly, effective overall organizational security.
Learn More
To learn more about security services, or to determine if a mobile security assessment is right for your organization, contact your Verizon Business account manager, or visit verizonbusiness.com.

1. Guidelines on Cell Phone and PDA Security: Recommendations of the National Institute of Standards and Technology. Published by National Institute of Standards and Technology – U.S. Department of Commerce

Microsoft and Outlook are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

About Verizon Business
Verizon Business, a unit of Verizon Communications (NYSE: VZ), is a global leader in communications and IT solutions. We combine professional expertise with one of the world’s most connected IP networks to deliver award-winning communications, IT, information security and network solutions. We securely connect today’s extended enterprises of widespread and mobile customers, partners, suppliers and employees—enabling them to increase productivity and efficiency and help preserve the environment. Many of the world’s largest businesses and governments—including 96 percent of the Fortune 1000 and thousands of government agencies and educational institutions—rely on our professional and managed services and network technologies to accelerate their business. Find out more at www.verizonbusiness.com.