# Business Risks and Security Assessment for Mobile Devices

PATRICIA MAYER MILLIGAN
Information Systems Department
Baylor University
Waco, Texas
USA
http://business.baylor.edu/pati_milligan/

DONNA HUTCHESON
Director of It Audit
TXU Corporation
Dallas, Texas
USA
http://www.txu.com

*Abstract:* - Technology advances over the past decade have elevated business risk from mobile devices to an unparalleled high. The relationships between security, business risks, and their corresponding costs are increasingly complex. Corporate security measures have lagged behind the need for protection. Bottom line security relies on the individual business professional is ethics and diligence in protecting confidential corporate, market, and customer information. This paper identifies and compares the various business risks, assesses prevalent security solutions, and analyzes the total cost of corporate mobile technology.

*Key-Words:* - Security, Wireless, Smart phone threat, PDA threat, Network threat, Business risk, Malware

## 1 Introduction

Computing technology advances in the past decade have created a much more flexible corporate work environment. This flexibility is reflected in small mobile devices that are easy to use, provide the ability to receive and make phone calls and voice messages, send and receive emails and instant messages, access the intranet, surf the internet, and access business applications. These capabilities are available whether you are out of the office or out of the country. Wireless devices make geographic distance a non-issue. Flexibility is also reflected in extremely small mass storage devices. Up to 4 GB of data (equating to approximately 80,000 boxes of paper) can be as small as a pen.

Mobile technology has enabled greater productivity, availability, and convenience to business professionals and executives. Unfortunately, it has also enabled fraudulent and criminal behavior to be more easily accomplished. Business resiliency mandates adequate security measures to mitigate the risks inherent to using mobile technology. As we identify business risks and countermeasures, the term "security" is focused on preventing breaches and protecting corporate data. While security options for commercial corporations have lagged behind the availability of new technology and the need for protection, businesses will ultimately have to rely on the individual employees' ethics and due diligence in protecting confidential corporate, market, and customer information.

In the context of this paper the term "mobile devices" will include smart phones, personal digital assistant (PDA) devices (eg. Blackberry, Treo, Palm, pocket PC's), flash drives, memory sticks, and other RF and USB devices that enable remote access to business networks, the internet, and transfer of mass data to non-business equipment. For this paper, we do not include laptop/notebook personal computers.

## 2 Risks

Each of the risks listed below point to immature security solution options to mitigate the business risks. Corporations should note that no single golden bullet will eliminate all risks. Table 1 identifies categories of security threats and possible countermeasures.

### 2.1 Risks of using mobile devices

- Viruses, worms, or other PDA-specific malware
- Theft of sensitive data
- Exposure of critical information through wireless sniffers. Wireless intruders could capture emails,

email addresses and attached data if security is insufficient

- Loss, theft, or damage of device
- Use of the PDA as proxy to establish virtual connection from an attacker to an internal network
- Data loss/leakage due to the small footprint and portability
- Fraud enabled by remote access or copying mass amounts of sensitive data
- Spam causing disruption and driving up service costs if targeted toward mobile devices
- Malformed SMS messages causing device to crash.

| Applications | Security Threat | Countermeasure |
|---|---|---|
| Checking email | Viruses, worms, or other PDA-specific malware | Do not click on every link or open every attachment. Curiosity often overwhelms common sense.<br>View unsolicited messages with suspicion. No click, no virus.<br>Use anti-malware software.<br>Connect to service providers with firewalls.<br>Set options to prevent install of executable software on mobile device.<br>Beware of unexpected connections and update confirmations. |
| Personal information management (contacts, notes or memos, to do lists, calendars) | Theft of sensitive data | Encrypt data on storage device<br>At a minimum password protect flash drives and memory sticks<br>Disable Bluetooth feature if not used.<br>Do not set device as discoverable if using Bluetooth |
| Global communication | Loss or theft of device<br>Dedicated eavesdroppers invest a few thousand dollars for equipment which enables cracking GSM authentication protocols and reconstructing voice conversations and data messages with ease | Use remote access tools to wipe memory<br>When using VPN for sensitive data and high value targets, use direct SIP compliant VoIP clients. Acoustic Echo Channeling is not encryption. As described in FIPS 197, you should use the Advanced Encryption Standard (AES). |
| Access to business application | Proxy used to establish virtual connection from an attacker to an internal application<br>Malicious destruction of business data<br>Fraud enabled by remote access or copying mass amounts of sensitive data | Use firewalls to minimize access.<br>Prevent access privileges from wireless devices.<br>Use 2-level authentication for access.<br>At a minimum, password protect flash drives and memory sticks.<br>Encrypt data (use most current security level; WEP and EAP are no longer enough). |

Table 1

## 2.2 Inherent Security Issues for All Mobile Devices and Applications on the Mobile Devices

Many security issues inherent to mobile technology must have a well planned corporate approach to manage the issues and mitigate the business risk. The following list identifies some of these security issues:

- Threats differ by industry group (e.g. intelligence/ security/police forces, fuel and energy, health and disease control, transportation, media, financial, food, retail sales, consumers), therefore the countermeasures must appropriately match the threat.
- Businesses cannot manage what they cannot identify and track or measure.
- Some companies outsource network security. When the third party employees leave, what customer data leaves with them? Business data is available to providers with different business goals and objectives.
- Network Security Issues
    - Conventional firewall and VPN security systems are inadequate for wireless mobile devices
    - Lack of integration with WAN network security solutions
    - Blurred network perimeter
    - If communication can be intercepted, piggybacked, impersonated, re-routed to bad people, good people can look bad and bad people can look good from any location.
    - Encrypted remote connections are assumed secure because the data is encrypted. Little consideration is given to securing the end point (e.g. blackjacking). Note: email and other communications are encrypted only from phone to phone company or mobile device to server. Beyond that point, email, instant messages and file transfers maybe transmitted unencrypted over public internet (e.g. Consultant using own email address or phone on different carrier).
    - Ad-hoc service provisioning
- Device-specific Security Issues
    - USB device detection and authorization
    - Deleted files not really deleted, just like the laptop or desktop hard drive, a "recover file" program can bring back deleted files.
    - Hackers can pay $100 for a developer key for Research in Motion's Blackberry devices. This key enables the Blackberry to be used as a proxy. Corporations that use a Corporate Blackberry Enterprise Server, and disable 3rd party applications installations are not at risk (will not read .JAD files). Individuals who purchase Blackberry devices in retail, use public email service providers could be affected by this issue. The same issue may apply to all mobile devices.
- Government Regulations
    - Canada: PIPEDA, personally identifiable information (PII) transfer to other countries
    - USA: Gramm-Leach-Bliley, Sarbanes-Oxley, CA1386, HIPAA, PII/Customer Data Privacy, Electronic Data Discovery, and DoD Directive 1800.2
    - EU: Data Protection Directive
    - ISO 27001
    - OECD International Guidelines for Data Privacy and Trans-border Flows of Personal Data
- Common Malware
    - SNARF attack – access to stored data portions of the phone or other mobile equipment without owner's knowledge
    - Blackjacking – hacking into an enterprise system using a blackberry. The communications channel between the BlackBerry server and handheld device is encrypted and cannot be properly inspected by typical security products
    - Backdoor attack – Bluetooth pairing with mobile equipment in a "trusted relationship" when the relationship is unpaired the connect remains.
    - Blue bug – serial profile connection to device giving full access to the command set
    - Bluejacking – uses Bluetooth pairing protocol, a command message can be inserted in the "name" field. If the information exchange handshake is successful, then all data on the mobile device is available to the initiator.
- Data integrity for PDA's and smart phones relies upon synchronization with a stable fixed server system for backup and management.

Many common assumptions regarding mobile device security are inaccurate. All high value data and targets should be appropriately assessed for vulnerabilities and steps taken to prevent security breaches. Security breaches of ordinary business networks by someone from the outside are not as frequent as business employees unintentionally doing something that has security ramifications. Example: In January 2007 a large study in the UK tested the probability of corporate employees to introduce malware to the corporate networks. The consulting firm sent flash drives containing an anonymous message about "Party of a Lifetime". Percentages of people placing the flash drive in their computers connected to the corporate network varied by industry: 50% of finance directors, 65% media company employees, 38% of technology, retail and transportation companies' employees.

The key elements necessary for mobile device security are essentially the same as the past 20 years of technology security.

- Access Control – Mobile devices inherently lack physical access control. They are used in public places where risks of data loss, device loss, probing, and downloading data by unauthorized people are the highest.
- User authentication
- Data encryption
- Intrusion prevention
- Anti-virus, anti-malware
- Administrative standards and infrastructure
- Email security
- Network perimeter and transmission security

The most common security metrics used by corporations today in evaluating the adequacy of mobile device security include:

- Number of breaches or successful attacks
- Virus protection and frequency of virus definition updates
- Currency of patch management on the servers
- Compliance with federal regulations
- Cost of security solutions
- Cost of loss
- Evaluation of risk

Are these metrics sufficient? Do the corporations factor total cost of ownership into the equation? How do they measure the benefit and value of both the mobile devices and the security solutions? The total cost of operation/ownership is the sum of the following:

- Cost of the actual device
- Cost of the security components and server and software for managing mobile service
- Cost if device is loss or stolen.
- Negative publicity -- the price of a CNN moment.

So, how can security managers explain the value of incorporating adequate security? Have one failure that results in high profile theft or fraud.

## 3 Possible Security Improvements

No single security activity will address all of the security issues or business risks associated with mobile devices in the corporate environment. Table 2 offers some improvements to consider. The options were assimilated from research at 250 companies in the United States, Canada, UK, Europe, and India by CIO Magazine, PricewaterhouseCoopers, and personal in-depth interviews and audit research.

| Category | Security Improvement |
|---|---|
| Network-based | o Track rogue wireless devices by scanning for unauthorized device to desktop synchronization or for unauthorized devices accessing the network through the corporate wireless LAN<br>o Do not allow peer to peer wireless connection<br>o Implement controls for ad-hoc services<br>o Conduct real-time network audits |
| Server/Host-based | o Consider using a software product (ex. Credant Technologies Mobile Guardian) to detect devices trying to synchronize. The software can also set authentication regulation, encrypt data, disable potentially threatening programs, and purge data from lost or stolen devices.<br>o Implement role-based controls for host applications accessible from mobile devices. Consider device-id dependent access or copy permissions for the roles.<br>o Use USB detectors<br>o Isolate all servers facing the internet and all mail servers for PDAs in their own DMZs |
| Device-based | o Install anti-malware on each mobile device<br>o Require password to use<br>o Require access key to use<br>o Biometric access (retina scan, fingerprint, voice recognition) |

| | |
|---|---|
| General | o Implement policy for multiple erase of device or password after failed network/server login.<br>o Communicate threats and security activities to personnel. It is less likely that they will do the right things if never told what the right things are.<br>o Some researched companies disable USB ports – most business professionals think NO because the policy restricts use of or synchronization of many types of mobile devices. Some employees will find a way to work around the restriction, e.g. email files, web storage, thus circumventing the policy.<br>o Security activities should not materially hinder business. Therefore, the security group must understand business objectives.<br>o Mitigate all significant business risks through rapid identification, response, and correction procedures once breach occurs.<br>o Report trends |

Table 2

Security Models include global network systems for Fedex and UPS. The biggest decision a corporation will need to make with respect to mobile device security is the security level they are willing to pay for and support. If the total cost of the device and the risk it generates does not surpass the business benefit, the corporate management should “just say no.” Be sure to standardize on compatible equipment. Not all mobile devices share a common infrastructure. Multiple infrastructures increase costs at all levels: operation, maintenance/support, security, and servers.

## 4 What do we see in the future for mobile devices?

- Mobile device data encryption will be made mandatory at government agencies and other organizations that store customer/patient data. Senior executives concerned about potential public ridicule will demand that sensitive mobile data be protected.
- Expect new PDA’s to have encryption pre-installed at the factory.
- Theft of PDA’s and smart phones to grow significantly. The value and volume of data on the PDA will dictate the price.
- State and federal governments will pass more legislation governing the protection of customer information. If the requirements for data breach notification are reduced, loss of sensitive personal data from mobile devices will incur harsh penalties.
- Targeted attacks on military contractors and businesses with valuable customer information will increase.
- Smart phone and PDA-specific worms will successfully attack up to a million devices globally (greater than 200,000 in North America) by moving from phone to phone over wireless data networks. Adware profitability will be a trigger for attackers.
- Security researchers often exploit the wireless vulnerabilities prior to selling the information to manufacturers and service providers.

Future predictions were made based on trends identified by the Institute for Applied Network Security, Gartner, and Forrester. These companies survey leaders in cyber security development and corporate security executives each year to identify, then validate the current trends, which were most likely to happen, and which would have greatest impact if they did happen. Likelihood and impact constitute risk level.

## 5 Conclusion

With respect to mobile devices and security, business executives don’t know what the employees are doing, where the company is going, or what they should do. Information security and criminology are mature enough to know what to do about many common problems. What is relevant going forward is what is allowed to be relevant. The scope of mobile security problems could be limited in a stand alone company environment, but with world networks (and access by mobile devices to those world networks), everyone’s problems become ours too.