Enterprise Mobile Security

Trend Micro, Incorporated

Protecting Mobile Data and Increasing Productivity

A Trend Micro White Paper | November 2007

TABLE OF CONTENTS

INTRODUCTION

Today's smartphones and Personal Digital Assistants (PDAs) offer as much processing power and memory as PCs had a few years ago. Many of these mobile devices improve employee productivity by allowing employees ready access to needed information. While the devices may increase productivity and efficiency, they also bring new risks to organizations as confidential corporate and personal data can be lost when the device is misplaced or stolen. Other risks come in the form of malware infections, spam, and hacking of mobile devices.

Smartphones combine a full-featured mobile phone with personal computer-like functionality and processing power. Besides making phone calls, users can run applications, as well as access, store, and manipulate data from corporate networks and the Internet. Memory cards for these devices are approaching 8 GB capacity, providing ample space for storing enterprise data.

Software developers can now write applications on mobile platforms using a variety of software tools. The emerging open mobile platforms such as Symbian™ OS and Microsoft™ Windows™ Mobile enable applications to be installed by device owners without restriction.

Increased capacity, new applications, service offerings on both wide-area (cellular) and local-area (such as Wi-Fi) networks, and Bluetooth connectivity are contributing to the rapid adoption of mobile devices by business users.

Organizations are beginning to understand that securing mobile devices is as important as securing desktops and laptops. As with any major initiative, mobile device security management should address the business issue holistically by considering the combination of people, processes and technology.

This whitepaper discusses mobile security issues faced by organizations and provides IT executives with actionable mobile security best practices to mitigate those risks.

INCREASED USE OF MOBILE DEVICES IN THE WORKPLACE

According to IDC, the global mobile worker population will exceed 850 million in 2009[1] – representing more than one-quarter of the worldwide workforce. Both the projected rapid growth of smartphone shipments and their increasing use by employees will force organizations to consider their impact on enterprise security. (See Sidebar)

Employees use smartphones and PDAs to stay productive and transact important business without needing their PCs. In addition to the telephone functions, employees may use the devices to:

- Send and receive email
- Send and receive instant messages
- Use vertical applications
  - Enterprise Resource Planning (ERP)
  - Customer Resource Management (CRM)
  - Sales Force Automation (SFA)
- Scan barcodes
- Play on-line games
- Chat
- Browse Web pages
- Download and share files on the Internet
- Use Personal Information Management (PIM) functions and data such as contact information, and meeting agendas
- Store confidential personal and corporate data

In-Stat*: Smartphone Market Will Exceed Laptop Market for Next Five Years

- Smartphone shipments will grow at more than a 30% compound annual growth rate for the next five years globally
- The number of smartphones sold will exceed the number of laptops
- Smartphone use will grow mostly from use as a laptop replacement

All of these functions qualify the device to be treated as a serious platform with serious security risks for the company.

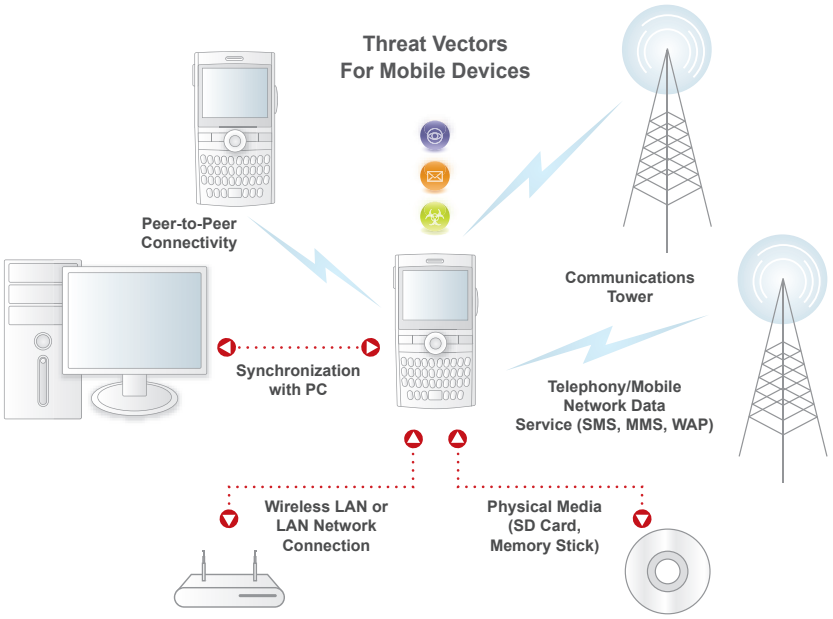
Companies are starting to access business applications such as Enterprise Resource Planning, Customer Relationship Management or Sales Force Automation on mobile devices. Mobile applications such as these can frequently include sensitive data on customers or business operations. Mobile applications also convert PDAs and mobile devices from an optional gadget into a critical business tool.

MAJOR SECURITY RISKS POSED BY MOBILE DEVICES

While mobile devices are productivity enhancing tools, they bring new security threats to the enterprise. A security breach on the device can be expensive to the organization.

The increasing numbers of mobile users and explosion of Internet connectivity have demolished the concept of a “fixed” perimeter for organizations. A company network protected by a central firewall is no longer adequate. Users frequently travel outside the perimeter, where they can expose confidential data and risk attacks. Mobile devices are at risk of carrying viruses and other malware, and release them into the network after the user reconnects behind the network firewall. Another downside of the portability of these compact computing devices is how easy they are to get lost or stolen, compromising the data accessed or stored on them.

1 IDC, Worldwide Mobile Worker Population 2005-2009 Forecast and Analysis, Doc #34124, Oct 2005
* In-Stat: Market Alert Email, and in “Smartphones 2007: The ARPU Generation Machine” (#IN0703823WH), November 2007



Major security risks due to mobile devices include:

- Loss of company confidential and intellectual property (IP) due to theft or loss of mobile devices
- Loss of employee productivity due to malware
- Loss of intellectual property due to spyware
- Fraud and lost productivity due to hacking

Each of the risks identified above are described in detail below.

Loss of Data on Mobile Devices

There will be eight million phones lost in 2007, including 700,000 smartphones, according to Bill Hughes, principal analyst at In-Stat, a technology research firm[2].

The cost of hardware and software of a lost device is trivial compared to the cost of information contained on the device. The lost data may lead to tarnished reputations, loss of competitive position, and potential litigation.

Customers, patients, investors, and business partners trust companies that deal with their sensitive information. Many governments around the world have enacted regulations that require companies to protect and manage data in accordance with that trust.

In the U.S., enterprises may need to comply with several regulations that include:

- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act, (SOX)
- Health Insurance Portability and Privacy Act (HIPPA)
- Government Information Security Reform Act (GRISA)
- Securities and Exchange Commission (SEC) Rule 17a-4
- Food and Drug Administration (FDA) Rule 11
- and multiple other laws protect consumers from release of personal, financial, and medical information

2 "8M cell phones will be lost in '07 - how to back yours up, Computerworld, July 13, 2007

The U.S. Government Information Security Reform Act (GISRA) requires enterprises to encrypt data and enforce authentication to protect sensitive government data.

European Union countries are governed by European Union Data Privacy Directive. Other nations such as Canada and Japan have similar regulations. All these laws carry severe penalties for releasing personal or corporate information. Along with the civil penalties for violation of these laws, the organizations face embarrassment and loss of faith.

When a device is lost or stolen, the data on the device is at risk of theft. So, organizations need ways to restrict access to the data resident on the mobile device. Unauthorized access to data can be thwarted by erasing or encrypting the data on the device. Data can be erased by issuing a remote erase command or by automatically erasing data upon a policy violation such as a number of failed login attempts. A remote erase command is not always effective because the erasure command will never be triggered if the device is not connected to the Internet or to the wireless carrier network. Encryption and policy driven data wipe solutions provide the best protection for data on the devices that are lost or stolen.

Finally, organizations need to have policies to recover devices that are currently not being used. Many users may choose to donate, sell, or throw away old phones as newer models are available. Data left undeleted on discarded phones will leave the company exposed to data theft and eventual regulatory violation lawsuits. While policies cannot completely eliminate all types of risks, it can make employees and managers aware and define steps to reduce the risk of data leakage, compliance violations, and embarrassing publicity for the company.

Loss of Employee Productivity Due to Malware

While viruses and worms are commonplace in PCs today, the growing population and capabilities of smartphone-class devices are expected to make these devices an appealing target for malware authors. The prospect of malware on mobile devices raises significant business issues and new security concerns.

> The built-in email and text messaging capabilities of smartphones make them a natural target for viruses.

One of the first significant attacks involving mobile phones occurred in June 2000 and focused on a specific mobile operator. Since then, viruses and malware have impacted the most popular mobile operating systems – Symbian OS, and Windows Mobile[3].

The built-in email and text messaging capabilities of smartphones make them a natural target for viruses. Greater connectivity brings with it larger propagation risks. Using built-in Wi-Fi and Bluetooth connectivity, malware can potentially spread by peer-to-peer communication between mobile devices.

A virus can leverage the phone's integrated messaging capabilities and PIM data to propagate to other phones. The Mabir virus propagated to other devices that support MMS text messaging by responding to received messages. In Spain, the CommWarrior virus was spread by sending itself to all the numbers found in the user's address book.

3 IDC, Worldwide Mobile Device Security 2007-20011 Forecast, Doc #206072, March 2007

Mobile malware also presents the prospect of financial loss due to fraud. Existing mobile malware affecting Symbian OS can send premium-rate messages without the user's knowledge. Future mobile spyware could use illicit tactics that already have proven success on PCs. Such fraud can increase business expenses and hinder productivity.

Short Message Service (SMS) spam consisting of junk text messages has been an issue in some regions of the world. Users can be distracted by junk SMS spam messages and can be manipulated into divulging confidential information by SMS-based phishing attacks, sometimes referred to as "smishing."

Loss of Intellectual Property Due to Spyware

The typical malware writer has shifted the intent of malware from pure fame and curiosity to criminal and financial gains. Malware is used to steal confidential data with an intent to sell it or cause harm to an organization. For example, Remote Access Trojans (RATS) and keyloggers may siphon out confidential information from a mobile device, just as they do on PCs and laptops.

Examples of mobile threats that can compromise business data include Acallno and Flexispy.

Acallno - In September 2006, spyware called Acallno was discovered that runs on Symbian devices. The spyware forwards all incoming and outgoing SMS messages to an external number. This allows the individual who installed the spyware to monitor SMS traffic sent and received by the victim.

Flexispy - In April 2006, commercial software called Flexispy came to market[4]. Flexispy has been positioned as helping people to eavesdrop on cheating partners. The application can be used to remotely activate the device microphone to listen to conversations. While it can be used to monitor spouses and wayward children, it also has the potential for use as a corporate espionage tool. Flexispy software sends out log information from the device to a central server without the owner's knowledge. A potential hacker would need to have physical access to a device to install the software. Once the software is installed, the hacker can read confidential messages, examine logs from any computer connected to the Internet, and listen to conversations.

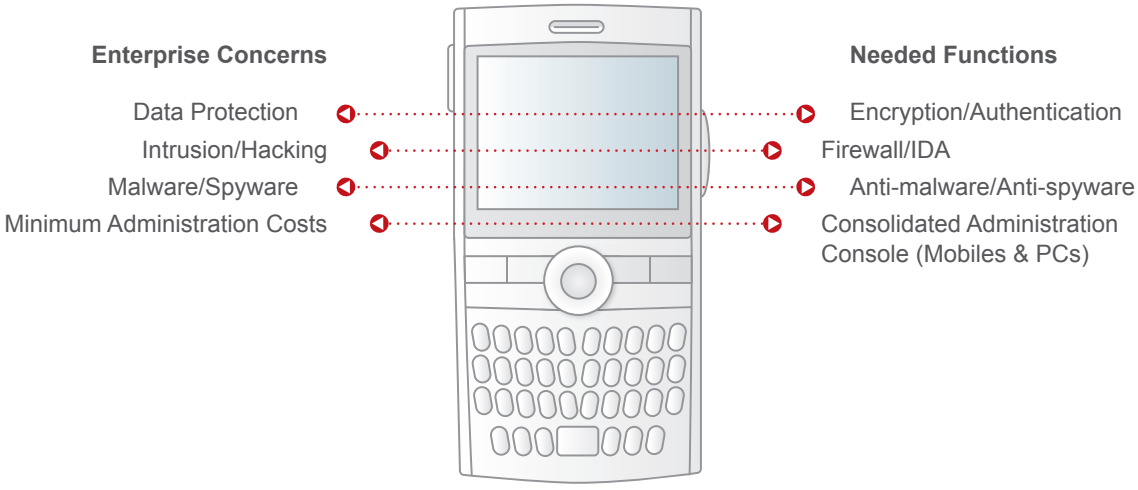
Fraud and Lost Productivity Due to Hacking

In addition to threats posed by malware, spam, and undesirable content, mobile devices are also likely targets for hacking and denial of service attacks Viruses take advantage of operating system vulnerabilities to launch attacks. For example, a malware called Skulls deactivates all links to applications on the mobile device. Once the device is infected with this malware, users cannot send email or instant messages, and calendar functions stop working. All the icons on the phone are replaced with skull images.

While the above mentioned risks might seem daunting, they can be mitigated by following some industry best practices. The following section describes suggested best practices by IT administrator to protect mobile devices from security related risks.

4 IDC, Worldwide Mobile Device Security 2007-20011 Forecast, Doc #206072, March 2007

BEST PRACTICES TO SECURE MOBILE DEVICES



Mobile Device Security Concerns and Technology Solutions

Technology is only a part of the mobile security picture. Security is typically a product of people, processes and technology. All these elements need to be considered to achieve the most robust security possible. To protect mobile devices and corporate networks from data and productivity loss, organizations should consider the following best practices:

- Establish clear policies for use of mobile devices
- Authenticate users and devices for data access
- Encrypt data at rest
- Secure connections for data in transit
- Install anti-malware protection on mobile devices
- Enforce firewall and intrusion detection systems (IDS) rules to deter hacking and denial of service attacks
- Centralize management of mobile devices security
- Improve user risk awareness and training

Establish Clear Policies for Use of Mobile Devices

Organizations need to consider legal and compliance-related issues for allowing mobile devices in their operations. Policies cannot be created in isolation but should be coordinated with cross-functional teams that include IT, purchasing, human resources, and legal departments.

"IDC expects worldwide shipments of corporate-liable converged mobile devices to experience a compound annual growth rate (CAGR) of 54% to reach over 82 million units shipped for 2011[5]." While the number of enterprise-owned devices is increasing, more and more users are also bringing their own devices to work. To control security risks, enterprise IT needs to set clear policies on the usage of mobile devices, no matter who owns them, and control the enterprise information accessed with these devices.

5 Cozza, Roberta "Report highlight for Dataquest insight: worldwide PDA and Smartphone shipments grow 26% in 1Q07" June 2007: ID Number G00149748

Knowing what type and model of devices are being used in the organization is essential to creating a viable security policy. Increased visibility into the device types and capabilities can help the administrator understand security exposure so that good policy decisions can be taken to protect corporate assets.

Some devices offer data synchronization from PCs to devices. Data synchronization ensures that critical data on the PC is downloaded and synchronized to the device from application such as Outlook or file storage. Most users like the productivity gains from synchronizing their mobile devices with their laptops.

> "IDC expects worldwide shipments of corporate-liable converged mobile devices to experience a compound annual growth rate (CAGR) of 54% to reach over 82 million units shipped for 2011[6]."

However, by using synchronization tools the users punch a hole in the enterprise security policy. Data that was secure on PCs has the potential to leak from unsecured mobile devices. The perimeter security and security policies for PCs, laptops, and servers may create a false sense of security for enterprise IT. IT administrators should consider restricting the use of synchronization to reduce the chance of malware being propagated or data lost.

In the event synchronization is allowed by the corporate policy, enterprises should consider the following steps:

- Educate users about risks and to recognize malware symptoms
- Secure devices against theft/loss to the same extent as a laptop
- Only synchronize essential files instead of synchronizing all files

Finally, not all data is needed by all users. A good content management policy should restrict access to data so that it is distributed only on as-needed basis.

> Tips for Mobile Device Security Policy

Establishing mobile device security policies helps secure data and protect productivity.

- Develop and enforce policies with an interdepartmental team that includes IT, purchasing, human resources, and legal departments.
- Know the type and model of device use to access or store corporate data
- Protect and restrict data synched to mobile device

Authenticate Users and Devices for Data Access

Mobile devices data need to be protected from access by unauthorized users. Password protection is a barrier to data access that every administrator should enforce in their networks. Mobile devices should have a power-on-password enabled so that the user is identified with the device.

Central management and enforcement eases the administrative burden of managing a password policy across all the users. Ideally, an IT administrator should be able to set global policies that apply to all devices from a single location.

A robust mobile security solution should enable administrators to establish and enforce policies consistently across all the devices. For example, an administrator should be able to prevent brute force logon attempts (multiple attempts with different login/password combinations). The administrator should be able to choose how to respond to multiple logon failures such as:

- restart the handheld device, then requiring user to provide the power-on password to continue
- require administrative logon to unlock the device
- delete all data from the handheld device as well as on any inserted memory card and restore the device to the factory default setting.

For maximum protection, data should be able to be wiped using software and pre-set conditions stored on the device. With this capability, data can be wiped even if the device radio is off and unreachable by the administrator.

> Tips for Mobile Authentication

Stop unauthorized data access with password protection

- Require power-on passwords on the mobile device
- Authenticate both device and user
- Select solutions with centralized policy management and enforcement

Encrypt Data at Rest

Encryption provides the most effective way to protect data at rest and is also the first line of defense against loss or theft of the device. Several states in the U.S. require companies to fully disclose the extent of the breach when data is lost. For example, California SB 1386 requires the breached organization to inform individuals that their information is compromised. Other countries have similar laws. In Japan, the breached organization has to disclose the breach to the government. The only exception to the full disclosure law is when the data is encrypted or if the company stopped the breach before the information was wrongfully acquired.

Some email solutions encrypt their mail storage. However, a comprehensive solution should include not only the mail storage but also the option to encrypt the rest of the data on the mobile device such as contact information, calendars, and files. Encryption should extend to files on the storage media used in the mobile device. An administrator should be able to configure the types of data to encrypt and the encryption algorithm to be used.

Several states in the U.S. require companies to fully disclosure the extent of the breach when data is lost.

The strength of any encryption system lies in the algorithm used. There are many algorithms available in the market. The choice of the algorithm can be distilled down to two types - secret key and public key algorithms. Secret key algorithms provide confidentiality whereas public key algorithms provide both authentication and confidentiality. Secret key algorithms are usually faster, often more than 1,000 times faster, than public key algorithms. Often, secret keys are used after some basic authentication is performed.

The most popular secret key algorithms are Advanced Encryption Standard (AES) and the older Triple Data Encryption Standard (3DES). Companies can balance government regulatory requirements with performance and resource issues if they have the choice of algorithm and key length. For example, some U.S. government organizations need higher key lengths to protect their most valuable data assets. However,

higher encryption keys consume more power, thus reducing battery life. An IT administrator should look for encryption solutions that offer flexibility such as 3DES and AES with 128 bit, 192 bit, and 256 bit encryption keys. The best implementation choice is to use the minimum strength encryption to achieve policy compliance. Using encryption that is stronger than required will negatively impact the device performance for the user.

Certified encryption solutions offer some security guarantees. Products that conform to Federal Information Processing Standards (FIPS 140-2) certification ensure that the data protection meets certain security requirements such as basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, and algorithm.

While full-device encryption is possible, companies should consider what information is necessary to encrypt. Encryption technology consumes valuable CPU, memory and battery resources. Encrypting only what is necessary minimizes such resource consumption.

Encryption solutions can be either "in place" or "container based." Some solutions that allow "in place" real-time encryption of files provide security without user intervention. However, folder or "container-based" encryption relies on user cooperation to protect data. Folder or container-based encryption leaves open the possibility that a user might accidentally save a confidential file outside of the container inviting the potential for policy non-compliance and data leaks.

Robust solutions should encrypt data on internal storage as well as on storage cards according to policies defined in a central management console. The central management console ideally should have processes to restore data access if and when users forget their encryption PIN and/or password.

A comprehensive solution should include encryption that meets appropriate standards and certifications (e.g. FIPS 140-2), provide flexibility in the choice of algorithm and the length of keys, and be able to safely retrieve data through key management.

> Tips for Mobile Data Encryption

Select data encryption that protects data to meet your policy, yet does not incur too high of a performance impact.

- Encrypt data at rest on mobile devices, including on storage media
- Select the minimum encryption necessary to comply with policy
- Choose certified encryption (i.e. FIPS 140-2) for better protection
- Use solutions that encrypt "in place" rather than containers, so data is protected without user intervention
- Manage encryption keys to protect them from theft

Secure Connections for Data in Transit

While the data at rest on a device needs to be encrypted, data in transit (emailed, accessed via wireless applications, etc.) also needs to be protected. By securing data in transit, data is protected from tampering by hackers during transmission from the device to the server. Secure Socket Layer (SSL) is a security protocol that ensures data is securely transmitted from the device to the server over a secure Web connection. SSL has become very popular because of its simple implementation and ease of use. Using SSL does not require new client software to be installed on the device.

Alternatively, VPN solutions can be used to secure data in motion. However, VPN solutions can be relatively expensive and may cause increased CPU utilization and battery drain on the mobile device due to processing of additional VPN client software on the device.

> Tips for Mobile Secure Connections

Data emailed or accessed via the mobile device can be tampered with unless protected.

- SSL protects data in transit, is simple to implement, and does not require new client software on mobile devices.
- VPNs can secure data in transit, but can be expensive, drain battery life, and require client software.

Install Malware Protection on Mobile Devices

Organizations need to consider protecting mobile devices just as they protect desktops and laptops. Mobile devices operate on networks that are beyond the enterprise perimeter. But when they connect back to the network, they may infect the IT systems. To provide mobile devices with equivalent protection to that on desktops and laptops, mobile devices need anti-malware software to limit the likelihood of infection.

To provide mobile devices with equivalent protection to that on desktops and laptops, mobile devices need anti-malware software to limit the likelihood of infection.

Anti-malware software watches for known patterns or behaviors exhibited by viruses, worms, Trojans, spyware, and other unauthorized programs. When malware gets installed on the mobile device, it not only can siphon off confidential information, but also can lead to lost productivity and increased support costs.

Anti-malware solutions scan for mobile threats and block them from installing on the device. Some commercial applications such as Flexispy might have legitimate uses. However, the user should be made aware that such a program exists and the user should be given an option to delete it.

To be most effective, anti-malware and anti-spam solutions should receive regular updates of new patterns for known malware with minimum user or administrative intervention.

Mobile data should be scanned in real time. This includes data on mobile devices and on external memory cards when inserted. If needed, the administrator should be able to schedule a manual scan on one or more devices. The solution also should be able to scan specific file types and compressed files such as ZIP and CAB formats.

> Tips for Mobile Anti-Malware

Provide PC-equivalent protection for mobile devices.

- Scan for mobile threats and applications
- Solutions should get regular updates with minimum user or administrator intervention
- Scan for malware in real time on devices and storage media

Enforce Active Firewall and Intrusion Detection Systems

In the same way that PC security solutions typically include a firewall to restrict access, mobile devices also need firewall protection. Firewalls have stateful inspection capabilities. When activated, firewalls limit the type and origins of traffic. Personal firewalls are necessary to block port scans that attackers may use to determine vulnerabilities when the device is connected to a public network. They also are the first line of defense against any exploitation of unpatched security holes in an operating system or client applications..

Organizations typically need firewall and intrusion detection systems with predefined security levels that can be further customized by the administrator. Using a centralized management console, the IT administrator should be able to filter traffic from a specific IP address, port number, or protocol. An intrusion detection system (IDS) when implemented on a mobile device can block denial of service attacks on the mobile device by identifying patterns in network traffic.

The optimal solution should have an easy-to-use interface to set policies such as block or allow all inbound, outbound, or both inbound and outbound traffic.

The administrator should be able to choose from a default security level such as:

- "Low" to allow all inbound and outbound traffic
- "Medium" to allow all outbound traffic but block all inbound traffic
- "High" to block all inbound and outbound traffic

The solution should also allow the administrator to set an exception list to override security level settings or block certain types of network traffic. For example, administrators should be able to exclude some protocols, ports, and IP addresses from inspection as there will be different requirements for users at different levels in the organization.

> Tips for Firewall and Intrusion Detection Systems

Inspecting and restricting access to devices improves mobile device security.

- Firewalls limit the type and origin of traffic.
- Select easy-to-deploy firewall solutions with pre-defined security levels that are customizable by the administrator.
- Intrusion detection systems can block denial of service attacks.

Centralize Management for Mobile Device Security

Centralized management reduces complexity and cost of managing multiple devices. Mobile devices are by definition routinely outside the organization, so any solution that does not enable remote management and policy enforcement for these devices may be inadequate. These tools ensure that all mobile devices contain the same version of the same software and removes applications that are unauthorized. Software distribution is also a critical element in the mobile data protection strategy.

> Tips for Central Management of Mobile Security

From a central Web management console, an IT administrator should be able to:

- install the mobile security application(s) on the handsets
- centralize provisioning of settings and policies
- lock mobile security settings on the device so users cannot modify them
- push software patch updates, security and pattern file updates to the mobile device

Data on the device should be wiped when certain conditions occur, such as too many unsuccessful logins. The data wipe should be successful even if the device is set in "flight mode" or disconnected from wireless network by disabling the device radio. The management console should be able to set data wipe policy so that the security software resident on the device can check for these administrator-set conditions and wipe the data from the device when those policies are violated. This unconnected "remote wipe" helps protect data even if a thief removes the SIM (Subscriber Identity Module) or turns off the wireless connection.

Event logs should be available so reports on the threats faced by the organization can be created and viewed to better manage risk.

Many organizations have device management tools. The solution should work with the existing device management tools deployed in the network.

Finally, organizations will reduce operational and capital expenses as well as get a better view of their data security and compliance if they can manage enterprise desktop and mobile device security solutions from a single console.

Improve User Awareness and Training

Improving security protection involves considering people and processes along with technology, and includes comprehensive training to communicate the threats posed to networks through the use of mobile devices. Just as PC users recognize spam and phishing, mobile users also need to recognize the potential threats on their devices.

> Tips to Educate Users

Users should be educated to follow corporate policies for safe use of mobile devices.

Some of the recommended safe practices are:

- do not download applications from untrusted sources
- do not share applications with strangers
- do not keep Bluetooth functionality enabled when not in use
- do backup all data on the device
- do keep the software on the device up to date (OS patches, anti-virus signatures, firewall settings, etc.)
- follow tips for safe synchronization

CONCLUSION

Many large and small businesses provide their employees with smartphones and PDAs to increase employee productivity. Although they boost employee productivity, mobile devices create security challenges for organizations.

Organizations should view mobile security holistically – people, processes, and technology – to mitigate risks. A comprehensive solution includes training people to use mobile devices safely, extending desktop and laptop security policies to mobile devices, and implementing mobile security technology solutions.

Users have to be trained to use their mobile devices safely. Many of the common sense practices applied to PCs and laptops are applicable to mobile devices as well. Just as users avoid malicious web sites on their desktops, employees should be cautious while surfing the Internet on their mobile devices. A consistent policy across all IT assets increases the chances of keeping the organization secure from threats. The IT administrator should extend the security practices used for laptops and desktops to mobile devices as the security risks are the same for both.

Finally, organizations should consider mobile security technologies that include authentication, encryption of stored data, security for data in transit, anti-malware, firewall and intrusion detection systems, and centralized management to protect both mobile devices and the IT network from security risks.

Mobile device security should and can be managed very much like PC security. By training employees, developing mobile security policies, and selecting flexible yet comprehensive security technology, mobile devices can be deployed in the organizations to increase productivity of its employees.

TREND MICRO™ MOBILE SECURITY

Trend Micro Mobile Security protects smartphones and PDAs from data loss, infections, and attacks. Its central enterprise console can also manage desktop protection. Encryption and authentication defends data integrity on lost or stolen devices. The anti-malware features block viruses, worms, Trojans, and SMS text message spam. Built-in firewall and IDS protects against hackers, intrusions, and denial-of-service attacks—potential threats to the increasing number of Wi-Fi-enabled mobile devices.

Advantages of Trend Micro™ Mobile Security

- Secures information against accidental loss
- Improves protection while reducing complexity
- Reduces administration with integrated management
- Maintains mobile worker productivity

Learn more at www.trendmicro.com/mobilesecurity.

TREND MICRO INC.

10101 N. De Anza Blvd.
Cupertino, CA 95014

US toll free: 1 +800.228.5651
phone: 1 +408.257.1500
fax: 1 +408.257.2003

www.trendmicro.com