



Seven Tips for Securing Mobile Workers

Sponsored by Sophos

Published by Ponemon Institute LLC

Publication Date: May 2011

Seven Tips for Securing Mobile Workers

Ponemon Institute, May 2011

Part 1. Introduction

Seven Tips for Securing Mobile Workers is intended to offer practical guidance on dealing with one of the fastest growing threats to the security of sensitive and confidential information. It is the increasing sophistication and convenience of such mobile devices as laptops, Androids, iPads and USB sticks that contribute to both their popularity in the workplace and their risk to an organization's networks, data and reputation.

The security of connected mobile devices in the workplace is important to an organization's security strategy because data breaches involving lost or stolen laptop computers or other mobile data-bearing devices remain a consistent and expensive threat. According to Ponemon Institute's *2010 Annual Cost of a Data Breach Study*, 35 percent of organizations report that a lost or stolen mobile device caused the data breach they experienced.¹

Further, while the average cost of a data breach in our annual study was \$214 per lost or stolen record, a data breach involving a lost or stolen mobile device was \$258 per record. Our research suggests that device-related breaches have consistently cost more than many other types of data breaches. This may be because investigations and forensics into lost or stolen devices can be more difficult and costly.

Some security experts² have now designated smartphones and other mobile devices as an organization's most serious threat vector. The reason is due in part to the nomadic work life of an organization's employees. Sensitive data on mobile devices travels from the office to home and other off-site locations. According to Ponemon Institute's security tracking study of 116 organizations, it was revealed that in these organizations 62 percent of mobile data bearing devices that were lost or stolen did, in fact, contain sensitive or confidential information.³

In the course of their daily work life, employees frequently use mobile devices such as laptops and smartphones for both business and personal reasons. Thus, sensitive business and personal information is co-mingled on these devices. In a recent study on smartphone security, we found that 40 percent of consumers surveyed use their smartphone for both business and personal use equally and 25 percent use it for personal but some business use.⁴

Sixty-six percent of consumers in this study store a moderate or significant amount of personal data. Most often these include email addresses, names, contact lists, photos, anniversary and other personal dates and locations. Typically employees use their smartphones for business phone calls, Internet browsing, corporate email, credit or debit card payments, customer relationship management, travel assistance, contact management and business social networking, video conferencing, scheduling tasks and reading documents. In some cases, workflow applications are run on a smartphone such as filling in forms as part of an employee task.⁵

Employees also can be careless when using smartphones while in public places. In a study Ponemon Institute conducted on the security of voice data, we learned that the interception of corporate secrets during smartphone conversations is costly and not likely to be discovered.

¹ *2010 Annual Cost of a Data Breach: US Study*, Ponemon Institute (sponsored by Symantec), March 2011

² Dr. Larry Ponemon and Stanton Gatewood, *Ponemon's Predictions: Trends in IT Security*, Webinar sponsored by ArcSight, May 17, 2011

³ Ponemon Institute's security tracking study of 116 global companies with a special carve-out on mobile-connected devices used by employees, conducted September 2010 through March 2011

⁴ *Ibid*, Footnote 3

⁵ *Smartphone Security: Survey of U.S. Consumers*, conducted by Ponemon Institute (sponsored by AVG), March 2011

According to the study, the average cost to an organization every time a corporate secret is revealed to unauthorized parties, especially agents and their competitors, is \$1.3 million. Forty-three percent of respondents believe this occurs about once every month and 29 percent believe it happens annually. Eighty percent believe that the organization would not discover the wrongful interception of a smartphone conversation that revealed valuable corporate secrets.⁶

Other vulnerabilities these devices face include attacks by viruses, spyware, malicious downloads, phishing and spam. It also has been found that Androids and iPhones have emerged as popular platforms for attack. There also has been a consistent degree of evolution in the sophistication and execution of these threats.⁷

Part 2. Tips for Securing Mobile Workers

To help address these risks, we have identified seven key areas where organizations can make improvements to the security of their mobile workers. Where applicable, we use cases from actual data breach incidents to illustrate these risks. These cases are based on interviews conducted in organizations that have participated in our annual *Cost of a Data Breach* studies.

Tip 1. Develop an enterprise strategy for mobile security. Our research suggests that mobile security creates new challenges for IT and IT security practitioners, which demand a holistic or strategic approach to managing risks, threats and vulnerabilities without diminishing user convenience or productivity.

The solution is not to limit the use of these devices but to accept the fact that mobile devices are now a way of life. Mobile devices increase the efficiency of workers, flexibility and speed in deploying new applications, increased end-user convenience and decreased operating costs.

To create an enterprise strategy we recommend conducting an audit to determine where laptops and other mobile devices are used within the organization. As reducing the number of devices based on which employees really need them to work effectively is unrealistic in most organizations, an audit helps to understand the level of risk and enabling technologies that limit access to or transfer of sensitive and confidential information.

We also suggest classifying the sensitive data employees have on these devices. Data can be classified as follows: regulated data (such as credit cards, health data, SSN and driver's license number), non-regulated customer data (such as purchase history, email address list, shipping information), non-regulated confidential business data (such as IP, business plans and financial records) and employee data.

Based on this classification, make sure appropriate safeguards are in place and that employees understand they are also accountable for the data's security. Conduct a risk assessment to determine possible theft scenarios for the data stored, processed, or transmitted by these devices. Devise appropriate security measures to protect both the data and the laptop. Finally, create a lost mobile device response team to monitor laptops, smartphones and other mobile devices.

Tip 2. 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. Guidelines can range from such topics as to what types of data should not be stored on these devices, how to determine if an application can be safely downloaded and how to report a lost or stolen device.

⁶ The Security of Voice Data, Ponemon Institute (sponsored by Cellcrypt) April 2010

⁷ Global Security Insight for Mobile, published by Adaptivemobile, February 2011

In addition, establish rigorous monitoring practices and implement enabling technologies to ensure policies and guidelines are strictly enforced.

Comprehensive security policies may be a challenge to create and enforce because of the variety and number of mobile devices in use. For this reason we recommend, as discussed in our first recommendation, taking an inventory of the devices and the types of data that is stored on them.

One area that definitely needs to be addressed in policies is the practice of turning off security settings or “jailbreaking.” Ponemon Institute tracking study of 116 companies revealed that two-thirds of these companies report that 10 percent or more of their employees routinely turn-off or disengage the security features on their mobile devices. This practice has been shown to be a pervasive problem within companies.⁸

The following case illustrates the need to have policies for the acceptable use of mobile devices in the workplace, including making sure security settings are not turned off.

A physician assistant at one of the largest healthcare facilities in the metro New York area used an iPad containing detailed and sensitive information about her patients. Because she was on call 24 hours per day, the PA carried it at all times. One afternoon the PA stopped to have lunch and left the iPad in the car. When the PA was at lunch, a thief broke into the car and stole the iPad containing patient data. Unfortunately, the security settings were not turned on and the thief was able to access the medical credentials of more than 200 individuals.

As we mention above, it is important to validate that policies are being followed and employees are in compliance. Therefore, it is important to make sure that mechanisms are in place to detect non-compliance and punish negligent or malicious employees, such as in the following case of the sales associate who lost his job.

A sales associate in a large brokerage firm heard rumors that layoffs were imminent. Learning that he was about to be a victim of the downsizing, the sales associate decided to download the contact information of the wealthiest clients on his notebook computer. Weeks later the firm was inundated with calls from clients complaining about receiving unsolicited emails and letters from a competing firm.

Tip 3. Establish organizational accountability. Organizations have a responsibility to provide their employees with the policies, procedures and technologies necessary to 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.

As a starting point to creating employee awareness, organizations need to have a clear and concise policy that defines the employee’s responsibility and accountability. 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

The following case shows how the use of a smart device for both personal and business reasons can put an organization’s sensitive data at risk. According to our security tracking study, 91 percent of the companies say their employees downloaded web applications that contained malware, viruses, malicious code, botnets or worse.⁹

⁸ Ibid, Footnote 3

⁹ Ibid, Footnote 3

An employee of a retail company had a smartphone and used it for a variety of purposes. The employee liked a financial application to help manage bill paying and make purchases. The employee unknowingly downloaded a financial application that was infected with malware that resulted in the theft of credit card information. Three months later the employee received a credit card bill with thousands of dollars of purchases that were not made. In addition, the smartphone had information about the company's customers that could now be potentially at risk for a data breach.

As part of establishing employee accountability, conduct a risk assessment to determine possible theft scenarios for the data stored, processed, or transmitted by mobile devices and share these with employees. Devise appropriate security measures to protect both the data and the laptop. Implement the required protection strategies. Finally, create a lost device response team to monitor laptops, smartphones and other mobile devices.

Tip 4. Launch awareness training for end-users (to reduce employee mistakes). Beyond policies and monitoring of employee behaviors, organizations should implement a training program to help employees understand the new and emerging security threats present when they use their mobile device. Training programs should emphasize the need to be careful when transmitting confidential information. This is especially important because, as we mention earlier in the paper, employees are increasingly using business mobile devices for personal use as well.

Employees should be trained to recognize a phish. Inform them that phishing emails usually appear to come from well-known organizations and ask for personal and confidential information. Make sure employees understand that these threats are also targeting Web 2.0, social media and social networking sites.

Phishing attacks are just one the threats that can be used to steal business confidential information. The case below illustrates how employees can make mistakes that lead to a data breach.

An accountant in the human resources department of a manufacturing firm was responsible for assisting in the administration of employees' 401k plans. One morning, while working from home, the accountant opened an email on her laptop and without carefully reading it clicked open an attachment she believed was from one of the company's investment firms. She replied to the email and sent confidential information about the company's pension accounts. Weeks later the company learned that its pension fund had been hacked and employees' personal data stolen.

Another risk that employees need to be aware of is the vulnerability of voice data. Employees should be instructed never to assume voice calls are confidential (like fax or email), especially when calling internationally where some countries' phone operators have no encryption security in place at all. As we discuss earlier in this paper, an often overlooked risk to confidential information is the disclosure of IP and other sensitive business information during phone conversations.

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 be advised to turn off Bluetooth if they are not using it. If employees strongly suspect their calls are being listened to then turn off the phone when it is not needed. Use encryption software that works worldwide to secure sensitive calls.

Tip 5. Use application control, patching and other controls to prevent hacking and surreptitious malware infections. In our opinion, blacklisting methods are not enough for determining permissible applications that can be downloaded by employees onto their mobile devices. 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 are

patched and up-to-date. 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 enabled. In addition, you also should restrict use of Exchange Active Sync or other email synchronization to user-owned devices that comply with your security policies such as minimum password length.

We also suggest controlling and monitoring the data traveling to your network. According to research conducted by Ponemon Institute, many IT professionals do not know whether their organizations permit clear text traffic when transmitting from host to host. Or, whether they have controls in place to inform them about third-party data transfers.

Tip 6. Whenever feasible, use remote wipe, mobile device encryption and anti-theft technologies to reduce data breach risk. Based on previous Ponemon Institute research completed in May 2009, the total economic impact of one lost laptop is \$49,256. We also found that encryption on average can reduce the cost of a lost laptop by more than \$20,000.¹⁰

As our research shows a lost or stolen mobile device that is encrypted is much less costly to the organization than a mobile device containing confidential or sensitive data in clear text. In addition to encryption, the organization should seriously consider anti-theft technologies that can be used to locate a lost device or prevent unauthorized 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. And, 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.

Tip 7. Understand emerging privacy issues inherent with mobile devices. While the focus of this paper concerns security, there are inherent privacy risks associated 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. We also recommend conducting privacy impact assessments that closely examine the privacy and data protection risks associated with mobile devices.

Security and privacy are both important to creating trusted relationships with individuals. According to Ponemon Institute's 2010 Most Trusted Companies study, respondents said that the top two practices that contribute to trust are substantial security practices and accuracy of personal information collected and retained.

The following case involves employee information stored on mobile devices. This case illustrates how both security and privacy practices impact trust and reputation.

A vice president with a global manufacturing firm was recently relocated to one of the company's overseas offices. The overseas HR department was asked to review the VP's medical records to ensure medical coverage would continue. The US office informed the overseas office that the VP was recently diagnosed with multiple sclerosis, which was now in the medical records. The US HR manager downloaded the records on her iPad and decided to send them to the overseas HR manager as private and confidential. Instead she pulled up the global contact list of the company's directors throughout the world. The VP's illness was now known throughout the organization.

A second privacy issue concerns the use of employee-owned mobile devices in the workplace. There are enormous privacy issues for organizations that routinely scan mobile-connected devices to make sure they contain the appropriate security features or do not contain company-confidential information.

¹⁰ The Cost of a Lost Laptop, Ponemon Institute, (sponsored by Intel), February 9, 2009

Outsourcing data to third parties creates another level of data protection and privacy risk for the organization. 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.

Finally, make sure that promises made to customers and employees about the use of their sensitive and personal information are kept. If these policies promise strict control over the transmission of sensitive information but these practices took place, the organization could face disgruntled customers, potential lawsuits and government fines. This also applies to promises regarding the collection and retention of personal information.

Part 3. Conclusion

The human factor risk, from both internal and external sources, poses a very real threat to mobile devices. We attempted to illustrate the risks through the cases we learned about in the course of conducting our annual data breach research.

Mobile devices are emerging as one of the most serious threat vectors in organizations. Their proliferation in the workplace creates an enormous challenge to the safeguarding of an organization's sensitive and confidential data. We believe the first step is to create an enterprise strategy for mobile security to be followed by the appropriate policies, procedures and technologies.

It is our observation that few organizations are putting in place policies for the secure use of mobile-connected devices. More than half (53 percent) of the 116 companies in our security tracking study have no policies and only 16 percent have a policy that applies to the entire enterprise.¹¹ We believe that the lack of implemented policies can be attributed to the speed at which new mobile devices are proliferating in the workplace, the difficulty in understanding the prevalence of mobile devices usage within an organization and the realization that their use is difficult to control and track in the workplace. New technologies are being developed to help in these areas.

Given the potential for a costly data breach and the loss of reputation due to the exposure of confidential information, we believe it is critical for companies to expand the focus of their data security initiatives to include mobile security. We hope that our seven tips provide high-level guidance on how to begin addressing this serious data protection risk.

¹¹ Ibid, Footnote 3

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.