Compliance Solutions for Mobile Device Computing: A Practical Guide for Compliance Officers

By Krista S. Zipfel, CFA

The Challenge

As a policy, Thomson Reuters used to issue Blackberry devices to its employees. Blackberrys were designed for the corporate world and became the smartphone of choice due to the security and central management features that Blackberrys offered. In 2010, Thomson Reuters started allowing employees to use their personal smartphones to synch up to the company's e-mail system in a belief that this policy would improve their ability to recruit talent or help morale. Today, they have several thousand devices connecting to the company's e-mail system and are finding management of this policy much more difficult than the central management and security of the company-owned Blackberry devices.[1]

Like Thomson Reuters, many financial services firms are embracing the "bring your own device" or BYOD phenomenon. Some companies believe that not having to issue company-owned devices will save them money, even if they offer to subsidize personal devices. They believe allowing employees to use their own devices to access company e-mail or other data will increase productivity and keep employees happy.

Increasingly employees are working from anywhere at any time and need constant access to company information. Mobile devices provide the means to work remotely and to access company information while on the go.

The problem with allowing the use of personal consumer devices is that they are not designed with corporate data security in mind; they operate outside the corporate firewall; and they may use means of sharing data that are not secure. The simple solution in the past was to prohibit the use of personal devices for company business; however, asking employees to carry two devices, their personal smartphone and a company-issued device, is becoming increasingly challenging. Try telling the CEO he may not send and receive company e-mail on his iPhone or the marketing department

Krista S. Zipfel is President and CEO of Advisor Solutions Group, Inc. (ASG), based in Newport Beach, California. ASG provides compliance and general business consulting services to small to mid-sized state and SEC registered investment advisers. Consulting services provided include assistance with registration, regulatory filings, development of compliance programs and written policies and procedures, mock audits and preparation for regulatory exams. Ms. Zipfel founded ASG in 2003 after a decade of working for registered investment advisory firms ranging in size from $50 million to $5 billion in assets under management, serving both retail and institutional clients. She has worked in the areas of compliance, portfolio management, client service, marketing, research, portfolio administration, operations, trading, and accounting.

they may not use an iPad to give presentations to clients and prospects.

The challenge for compliance and IT professionals at financial services firms is to develop a platform-independent approach to mobile device security management to address the growing array of mobile devices and the increased influence of employees in the choice of mobile devices. Mobile devices include: mobile/cellular phones; laptops/notebook/tablet computers; smartphones and PDAs; and any mobile device, including portable storage devices such as flash drives, that is capable of storing corporate data or connecting to the corporate or any unmanaged network. Whether firms mandate the use of company-owned devices or allow employees to use their own devices for company business, firms must implement policies, procedures, and controls that will address the risks these devices pose to nonpublic personal information and the firm.

Developing a mobile device management program requires the knowledge of mobile device security, information technology, and regulatory requirements. Developing the program must be a collaborative effort between compliance, IT and management.

In this article, I will address the current relevant regulations applicable to the use of mobile devices and the risks that the use of mobile devices pose to financial services firms. I will discuss that the solution to address those risks and meet regulatory requirements includes the adoption of comprehensive policies, and, if warranted and resources permit, implementation of a mobile device management solution.

The Regulations

Financial services firms should look to the compliance program, supervision, privacy, recordkeeping, and advertising regulations relevant to their firm in establishing policies and controls surrounding the use of mobile devices.

Under Rule 206(4)-7, investment advisers are required to adopt and implement written policies and procedures reasonably designed to prevent violations of the Investment Advisers Act of 1940 ("Advisers Act") and the rules thereunder, including among other things, implementing policies for safeguarding and keeping private client records and information.[2] Investment companies have similar requirements under Rule 38a-1 of the Investment Company Act of 1940. For broker-dealers, the applicable regulation is NASD Rule 3010, requiring firms to establish and maintain a system to supervise the activities of each associated person that is reasonably designed to achieve compliance with applicable federal securities laws and FINRA rules.

Additionally, Rule 30 under Regulation S-P requires every investment adviser, investment company and broker-dealer registered with the Commission to "adopt policies and procedures that address administrative, technical, and physical safeguards for protecting customer records and information. These policies and procedures must be reasonably designed to: (1) Insure the security and confidentiality of customer records and information; (2) Protect against any anticipated threats or hazards to the security or integrity of customer records and information; and (3) Protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer."[3] Given the state of technology today and the rapid advancements in technology and mobile devices, establishing and maintaining such policies will require compliance officers to develop and continually enhance their own technological knowledge as well as learn to work closely with technology experts.

Financial services firms must also look to applicable recordkeeping regulations in developing their policies. Mobile devices, in particular smartphones, are being used to retrieve and send company e-mail and text with clients or vendors. Advisers Act Rule 204-2(a)-7 requires investment advisers to maintain certain written communications. Rule 17a-4(b)(4) under the Securities Exchange Act of 1934 requires broker-dealers to maintain "originals of all communications received and copies of all communications sent (and any approvals thereof) by the member, broker or dealer (including inter-office memoranda and communications) relating to its business as such, including all communications which are subject to rules of a self-regulatory organization of which the member, broker or dealer is a member regarding communications with the public."[4] NASD Rule 3010(d)(3) requires retention of the business-related correspondence of registered representatives. According to the SEC, it is the content of an electronic communication that determines whether it must be preserved.[5]

To the extent associated persons use mobile devices for posting to social media sites, making client presentations, or updating company web sites, for example, financial services firms must be concerned with relevant advertising regulations, such as NASD Rule 2210(b)(2), NASD Rule 2211(b)(2), and Advisers Act Rule 204-2(a)(11), as well as recordkeeping rules.

Finally, compliance officers should be mindful that states may have adopted applicable laws as well. Certain states have adopted data security laws (e.g. MA and NV). Compliance should take those regulations into consideration to the extent the firm operates in one of those states or has clients in one of those states. Most states have also adopted laws surrounding reporting of data breaches. Visit the National Conference of State Legislatures web site for a list of state security breach notification laws.[6]

The Risks

The deployment of mobile devices without adequate policies, procedures and internal controls poses significant risks to financial services firms and their clients. The risks to individuals may include identity theft and theft or loss of financial assets, or embarrassment. The risks to firms may include a loss of public trust, legal liability, regulatory enforcement, costs to cure, or even blackmail.

By maintaining a strong information security program, which should include mobile device security, a firm can prevent or at least mitigate the risks of a security breach. Failing to have a strong program puts the firm at risk for security breaches as well as regulatory enforcement. Firms may be referred to enforcement even if there is no actual security breach or harm to a client. The lack of strong controls and therefore the risk of a security breach and potential that clients could be harmed are sufficient for a referral to enforcement.

Regulatory Risks

To date, there have not been any enforcement cases with respect to the use of mobile devices, such as smartphones or tablets, within financial services firms. However, given their rate of adoption, I believe it is only a matter of time. While not specifically involving mobile devices, the following cases illustrate violations of Rule 30(a) of Regulation S-P and related regulations, as well as the risks of failing to implement adequate policies, procedures and internal controls surrounding the use of technology. These cases provide important lessons on implementing policies involving mobile devices.

Lincoln Financial

The Financial Industry Regulatory Authority ("FINRA") fined Lincoln Financial Securities, Inc. and Lincoln Financial Advisors Corporation a combined $600,000 for violating Rule 30 of Regulation S-P and NASD and FINRA rules.

Between 2002 and 2009, the firms allowed employees to access their web-based customer account system by using one of two shared user names and passwords. The firms had no procedures to monitor the distribution of the common login credentials, were unable to determine which employees (current or former) had the login credentials, had no procedures to disable or change user names or passwords regularly or once associates left the firm, had not changed the shared credentials between 2002 and 2009, and had no means of determining who had accessed the web-based system or from where.

Additionally, the firms failed to require their registered representatives to utilize security software, such as antivirus, encryption, or firewall software, on their personal computers or to audit computers owned by their registered representatives and used in connection with firm business to determine whether they contained any kind of security application software.

Increasingly employees are working from anywhere at any time and need constant access to company information.

Failure by the firms in both of these areas put customer information at risk of being obtained through any number of hacking or intrusion schemes. As a result, the firms were found to have violated Rule 30 of Regulation S-P, NASD Rules 3010 and 2110 and FINRA Rule 2010.[7]

This case should be a lesson that, regardless of whether employees are allowed to use their personal desktop computers or their personal tablets to access

the company network and data, firms must apply the same procedures to both types of devices. Firms should practice good password management; they should require that all devices that connect to the company network utilize antivirus, encryption, and firewall protections; and firms must inspect those devices to ensure company policies are followed.

Commonwealth

In a similar case that lead to an actual breach of client information, in 2009, Commonwealth Financial Network ("Commonwealth") was found by the SEC to have willfully violated Rule 30(a) of Regulation S-P. Commonwealth, both a broker-dealer and investment adviser, recommended, but did not require, that its registered representatives maintain antivirus software on their computers, which the registered representatives used to access customer account information on the firm's internal network and clearing firm's trading platform. Commonwealth also did not have procedures in place to adequately review its registered representatives' computer security measures. In particular, Commonwealth did not audit branch office computers to determine whether antivirus software was installed, nor did Commonwealth have procedures in place to follow up on potential computer security issues.

In November 2008, an unauthorized party obtained the login credentials of a Commonwealth registered representative through the use of a computer virus placed on the registered representative's computer, which at the time did not have antivirus software properly employed, and was thereby able to access Commonwealth's internal network. The intruder accessed a list of the representative's Commonwealth customer accounts and entered unauthorized purchase orders in several of those accounts before the activity was detected by Commonwealth's clearing broker-dealer and the intruders were blocked from further trading.

In addition to the approximately $8,000 in net trading losses Commonwealth had to absorb, the SEC censured Commonwealth and ordered the firm to pay a monetary penalty of $100,000.[8]

The increased adoption of personal mobile devices to access company data coupled with the fact that mobile devices are more easily lost or stolen than desktop computers magnifies the risk that firms' data could be compromised via vulnerable devices and highlights the importance for the need for security policies for all devices accessing company data, including mobile devices.

Davidson

The final case particularly illustrates potential costs and serious implications to a firm and its clients when a firm fails to have adequate policies and controls. D.A. Davidson ("Davidson"), a broker-dealer, maintained a database server containing customer account numbers, social security numbers, names, addresses, dates of birth and certain other confidential data. Davidson did not encrypt or password-protect the database. In December 2007, the database was compromised when an unidentified third party downloaded the confidential data of 192,000 customers through a sophisticated network intrusion. The firm learned of the breach through an email that the hacker sent to the firm in January 2008 demanding a ransom for the data.

FINRA found that the firm had failed to adopt and implement policies and procedures reasonably designed to safeguard customer records and information and to establish and maintain a system, including written supervisory procedures, reasonably designed to achieve compliance with Rule 30 of Regulation S-P, NASD Rule 2110 and NASD Rules 3010(a) and (b).

The FINRA Letter of Acceptance, Waiver, and Consent shows the cost to the firm for this failure. Davidson took "prompt remedial steps after the hacker attacks, including issuing a press release to the public reporting the incident; preparing a detailed communication plan for employees, including establishing internal and external call centers to respond to customer inquiries; providing written notice to its affected customers; and voluntarily offering affected customers a subscription to a credit-monitoring service for a two year coverage period at a cost to the firm of $1.3 million." Davidson also resolved a class-action litigation with its affected customers, which included providing loss reimbursement for potential victims of the hacking of up to an aggregate of $1,000,000. Finally, Davidson also consented to being censured and fined $375,000.[9]

This case illustrates just how expensive a data breach can be and the importance of encrypting confidential customer data, regardless of whether

that data is maintained on the company network or a mobile device.

Computer Risks

To develop mobile device policies in an effort to prevent or mitigate regulatory and financial risks, firms must understand the technological vulnerabilities of mobiles devices. First, it is important to recognize that most mobile devices are computers and therefore present all the same risks associated with a desktop computer. Smartphones are not just phones with some additional features; they are computers with a phone. Mobile devices present all the same vulnerabilities to data leakage or hacking, but they also provide new opportunities for data loss and open potential new doors to allow hackers into the company network. Mobile devices should be subject to all of the same policies and controls implemented for the internal corporate network.

Like desktop computers, mobile device operating systems must be kept current to prevent vulnerabilities. While Microsoft and Apple have become very efficient at timely pushing out patches for newly discovered vulnerabilities for PCs, currently it can take cell phone carriers months to examine and approve a software update by the manufacturer, leaving devices vulnerable in the mean time.

Similarly, like desktops, mobile devices are at risk of becoming infected by and/or transmitting viruses or Trojans, worms, and spyware (collectively malware) and should be protected with antivirus and anti-malware applications. Mobile devices provide additional potential avenues for the company systems to become infected as mobile devices that become infected can transmit the viruses and malware to the corporate network when a connection is established.

While mobile devices have not seen as many threats as PCs, that statistic is likely to change as mobile device adoption grows. According to information technology market intelligence provider IDC, manufacturers shipped more smartphones than PCs to stores globally in the last three months of 2010.[10] In addition, the increasing amount of personal data that is being stored on these devices makes them attractive targets to data thieves.

Mobile devices that can browse the Internet pose all the same risks as desktops of downloading malware, but they add to the risk because they operate outside the company firewall. One way to address this risk is to use a software firewall on the device.

Cell phones are now also at risk from phishing scams. Cellular carriers are alerting their customers to phishing scams perpetrated via text message or unsolicited telephone calls.

Like devices in your network, mobile devices contain confidential, personal, sensitive, and company information, so they create a new avenue and risk to the potential loss of sensitive data. Like data in your network, data on mobile devices should be protected with strong passwords that are not shared and access should be removed once the person leaves the company. As with other electronic data, maintaining regular backups is critical. However, mobile devices containing and accessing data require additional controls to protect that information beyond what is needed to protect in-network data.

Additional Risks of Mobile Devices

While many mobile devices are computers and pose all of the same vulnerabilities as desktop computers, mobile devices pose many additional risks to the firm, and mobile devices that are not computers (e.g. USB drives) also expose the firm to data loss or theft. The primary challenge is that mobile devices are outside the company network accessing sensitive data that resides inside the network behind the protection of the company firewall. Additionally, the majority of mobile devices access company data not through a physical connection but via wireless fidelity ("Wi-Fi") or Bluetooth, which pose additional risks. Other features of mobile devices also pose their own unique risks.

Wireless Communications

One of the greatest risks of mobile devices is the means they use to communicate and connect with other devices. Whether they are connecting to the Internet through a cellular carrier, using Wi-Fi to connect to the company network, or using a Bluetooth headset, all of these communication methods create risks.

Wi-Fi is a mechanism for wirelessly connecting electronic devices. When a user is on the go, his or her mobile device uses public Wi-Fi, but public networks are not secure. Wi-Fi hotspots provide

free Internet connections in places like airports, hotels, and coffee shops. Hotspots pose significant security threats, such as sniffing and evil twin attacks. Sniffing uses a program that intercepts data to find specific information like passwords and credit card numbers. In an evil twin attack, a mobile device, such as a laptop or smartphone, is used to mirror the settings of a Wi-Fi hotspot to appear legitimate. Unsuspecting customers connect to this "rogue" Wi-Fi access point, which then allows the attacker to use sniffing technology to read data that the victim might be sending, including login IDs, passwords, and online account information. Also, some private Wi-Fi networks are not secure, such as a neighbor's Wi-Fi. If the employee can use the Wi-Fi connection without the permission and password from the neighbor, then anyone in the range of the network can intercept the communication that happens over that network.

Bluetooth is another wireless technology that allows Bluetooth-enabled devices to establish a wireless connection with other Bluetooth-enabled devices that are within a specified range. Bluetooth technology is used to pair headsets with cell phones, for example. Wireless data transmitted between Bluetooth-enabled devices is at risk of being intercepted, and hackers can use Bluetooth to download data without the user's knowledge. Smartphone malware can use Bluetooth to propagate.

The challenge for compliance and IT professionals at financial services firms is to develop a platform-independent approach to mobile device security management to address the growing array of mobile devices and the increased influence of employees in the choice of mobile devices.

Cellular communications at one time were unencrypted and easily intercepted. Today, cellular communication is much more secure and requires substantial sophistication and resources to be hacked. Therefore, cellular communication generally poses the least threat of data loss or theft of the three wireless communication methods.

Unique Risks

One of the unique risks of mobile devices is that they can be cracked via "rooting" a device running the Android operating system or "jailbreaking" a device running an Apple operating system. Cracking a device allows the user to bypass the security features of the device, thus potentially compromising both the device and its data. Users sometimes want to crack their device so that they can install unsigned applications, which are those that have not gone through the developer's testing process before being released to the market. Unsigned applications increase the risk of the device being infected with malware.

Applications on mobile devices create another unique risk in that they may be granted authority to use many or all of the features of the device, often without the user's awareness. Applications may access and use sensitive or substantial amounts of information contained on the devices, such as current location, phone number being called, or all of the contact data. They may be able to connect to and disconnect from Wi-Fi access points and make changes to configured Wi-Fi networks. They may be able to call phone numbers without the user's intervention. There are many legitimate applications that use these features and information for very legitimate purposes. However, even legitimate applications may collect vast amounts of sensitive data putting that data at risk of misuse. Furthermore, seemingly legitimate but malicious applications can use those same features to collect and share all of your contact data with third parties or erase all of your contact data, for example.

Also significant to mobile devices is their greater risk of being lost or stolen since they are small, portable, and used outside the company's physical confines. USB or thumb drives are incredibly small and easy to forget or lose, but laptops and cell phones are lost or stolen frequently as well. The loss of a mobile device brings with it not only the cost to replace the device, but it puts at risk sensitive data on the device and, if the device connects to the company network, any data that device is able to access. If the data on the device is not encrypted, the risk is increased. Even the financial services regulator is not immune to this

risk. According to an Office of Inspector General audit report of the U.S. Securities and Exchange Commission's encryption policy, the Commission had 15 security incidents in 2009 involving lost or stolen smartphones that were not encrypted. In one incident, a stolen, unencrypted smartphone was used to send a spoofed e-mail to the Commission Chairman, members of the press, and other media.[11]

Furthermore, many mobile devices have removable memory which provides an additional risk of loss of company data and another means for malware to be introduced to the company network. Hard drives can be removed from laptops to bypass password security to the device and gain direct access to the stored data. Removable memory cards in smartphones can be shared with other smartphone users, making the memory card vulnerable to a data breach or virus infection.

Finally, like all electronic data, mobile device data should be backed up regularly. Many mobile device backups are frequently unencrypted by default. This presents less of a problem if the backups are made to company computers that are protected. However, users of their own personal devices are likely to back them up to their personal computers, creating yet another copy of the device data that is outside the control and protection of the firm.

The Solution

The solution to a comprehensive mobile device compliance program is implementing a combination of appropriate policies, security features on mobile devices, and ideally an automated mobile device management and monitoring application. The challenge of implementing security policies is always balancing the need for security with the impact that security features and policy will have on the user's experience with the device.

Any solutions should be risk based, taking into consideration the nature of the access and the location of the confidential information. The more frequently data is accessed or the more people or devices allowed to access it, or if confidential data is transported offsite, the more opportunities there are for the data to be compromised and more robust controls are warranted. For more information on evaluating risks, see the publication issued last year by the National Institute of Standards and Technology of the U.S. Department of Commerce.[12]

Policies

Firms should develop comprehensive written policies and procedures for mobile device management. The policies should reflect the company's view on security and its policies for keeping company data safe and secure. Due to the shared risk of mobile devices with in-network computers, consider integrating mobile device policies with the firm's information security and privacy policies. Technology changes very rapidly, so create policies with flexibility that focus on the fundamental issues and general principals.

For all policies, consider and address the following questions: Who has access to data? What data do they have access to? Where are they accessing the data from? How are they accessing the data? What devices may they use? When can they access the data?

Firms may choose to prohibit or strictly limit how and what types of data can be accessed via mobile devices. Some firms may choose to restrict remote access to company data entirely so that the information will not leave the firm's physical boundaries. If access is permitted, the firm can establish policies and controls to ensure that the devices are properly secured and regularly test the devices to verify their security status.

Policies will generally fall into three categories: device, data and use, and monitoring and testing.

Device Policies

Device policies should address which devices are permitted for business use; protecting access to devices; enabling device settings; device maintenance; preventing and addressing the loss of a device; and the safe disposal of mobile devices.

Approved Devices – Company-issued vs. Employee-owned

Determine if the firm will allow the use of only company – issued devices or will permit the use of employee-owned devices. From a security standpoint, company-issued devices are easier to control and manage. If employee-owned devices are permitted to be used for business, bear in mind that management will be easier and the control will be greater the fewer types of devices permitted. In deciding whether to permit employee-owned devices, consider what types of devices employees want to use, what type of data employees want or

need to access, and what resources the firm has to control those devices.

Firms might adopt a two-tiered model, one that places greater limitations on personally owned devices than on company-issued devices. For example, Unisys permits employees to use their personal devices, but they must sign an acceptable-use policy that includes requiring employees to surrender their device at the request of Unisys for any investigation. Such a policy should complement and not replace a firm's comprehensive management and monitoring of personal devices. Additionally, the company limits what employees can access with their personal devices, such as e-mail or calendars. Employees can access more sensitive information by using a company-issued device that is current on patching and anti-virus and by using a secure connection.[13]

Solutions that will lead to what some people are calling "dual persona" mobile devices are in the very early stages of development. These solutions, using virtualization (the creation of a virtual, rather than actual, version of something), will allow a device to have two environments – a user environment and a work environment. Employees will be able to switch between the two environments, with only the work environment being managed by the business. This will be a way to insulate the company from the risks posed by the personal environment on the device.

For firms that permit the use of employee-owned devices to conduct company business and access the company network and company data, consider implementing the following policies. Regardless of whether a device is employee-owned, mandate that the employee and the device adhere to company policies. This may include the requirement that employees allow the firm to centrally manage the device, limit the applications they may use on the device, inspect the device regularly, and remove any company data and applications upon the employee's departure from the firm. Do not permit the use of "cracked," "rooted," or "jailbroken" phones. Have IT maintain a list of approved devices, devices that have been tested and meet the firm's security standards. Only permit the use of personal devices that are on the approved list. As new devices come on the market, have IT review and approve new devices and add them to the approved device list. Allow employees to submit requests for new devices to be added to the list; if they cannot be added provide an explanation to the employee why not and suggest alternatives with similar features. Policies surrounding employee-owned devices may need to be country specific, taking into consideration the privacy laws of the countries in which the company operates. For example, European laws restrict the degree to which companies can demand access to personal devices. Also, consider whether the firm will provide IT support to employee-owned devices. While IT should provide support related to the security and controls of the phone and use of any company-issued applications, providing general user support can be a significant drain on IT resources that should be focused on security and not helping employees download music to their phones. In considering the above-suggested policies, recognize the trade-offs between security and control on the one hand and flexibility, ease of use and employee morale on the other.

Device Access/User Authentication

The first line of defense to prevent unauthorized access to sensitive data and the company network via a mobile device is to control access to the device. Enable and require the use of the built-in password or PIN security of the device. This feature requires the user to enter a personal password or PIN before they can use or access data on the device. Many mobile devices also allow you to set the number of failed password attempts before the device is locked or performs a local wipe (deletion of data on the device).

Require the use of strong passwords. Strong passwords typically have a minimum of 10 characters; use a combination of at least three of the following four character sets: upper case, lower case, numbers, special characters; may not contain user identifiable information (such as the person's first, last, middle, a relative's, or pet's name or birth, anniversary or other relevant dates); and must be different for every account. Also, enable automatic password expiration so that users are required to change their passwords on a regular basis, e.g. every 60-90 days. Prohibit the use of shared passwords and implement policies and controls to remove access to company systems after termination.

Try to make use of multi-factor authentication where feasible. An authentication factor is a piece of information that is used to authenticate the identity of a person requesting access under

security constraints. Two-factor authentication is a security process wherein two different factors are used in conjunction to authenticate. The two factors typically include two of the following three methods: "something you know" (e.g. password or PIN), "something you have" (e.g. smartcard or token), or "something you are" (e.g. fingerprint or iris scan). Many laptop computers, for example, now have fingerprint readers that can be used in combination with a password.

Another feature to enable is the timeout feature that locks the device automatically after a certain period of inactivity. This prevents an unauthorized person from using the device after the user has already entered his/her password or PIN. Set that period of inactivity as short as is practical.

Device Settings

Establish policies on what device settings must be enabled. Mobile devices may have a number of configuration and security settings; however, often they must be enabled. Use built-in security features whenever available.

Device Maintenance

Firms should establish policies and procedures to keep mobile device operating systems updated and patched to prevent vulnerabilities in the same way that desktop operating systems should be kept patched. One difference is that the speed at which new devices are introduced and the sheer number of different devices is creating a challenge for security vendors to keep up patch-management software.

Additionally, just as the corporate network employs anti-virus and anti-malware applications to prevent viruses or other malware from infecting the corporate network, mobile devices should be protected with such applications. Be sure to enable automatic signature updates and perform automated regular scans of the device.

Device Protection and Loss

Maintain an inventory of all devices issued or used for company business and implement policies and controls to collect or disable all devices upon an employee's termination, whether voluntary or involuntary. Have a policy that all mobile devices should be treated like cash. Devices should never be left laying out in plain view. They should not be left in the car. Devices should never be left unattended for even the shortest amount of time when in public. Employees should know not to leave these devices sitting on a table at Starbucks while they go to the counter to get coffee or go to the restroom. They should not leave devices unattended at conferences or even sitting around on their desk at work. Mandate that mobile devices be carried in carry-on luggage and not in checked luggage.

Require that employees immediately report a lost or stolen portable device upon discovery. Losses should be reported to both compliance and IT as soon as practically possible. Consider using LoJack for laptops. This is laptop-tracking software that periodically phones home to the vendor's server to announce its location and to check and see if the laptop has been reported stolen. IT should disable access to the company's network by a lost or stolen device immediately and remotely lock and/or wipe the device. Report lost or stolen devices to the wireless carrier, if applicable, to disable the wireless capability.

Sale, Disposal, Separation

Have polices for the sanitizing of mobile devices or physical destruction of data devices. When wiping the data from the device, use a government or other high standard process that uses multiple passes using random data. If physically destroying the device, be sure to use a method that reasonably ensures the data cannot be recovered. If selling or donating an old laptop or cell phone, consider removing the hard drive or SIM chip and destroying them. Have policies for securely removing all company data from employee-owned devices and disabling remote access from those devices when employees leave the company or are terminated.

Data and Use Policies

Data and use policies should address what data may be stored on or accessed by the device; how to protect data on the device; whether network data may be accessed remotely by the device; what services and applications the device may use; and data backup and archiving policies.

Permitted Data

First, firms should establish policies on what data may be kept on mobile devices. The policies should take into account the type of device and the data

protections available on the device. Set policies on data that may be maintained on persistent (or device) memory or on memory cards (e.g. SD cards for smartphones).

Many companies may use mobile devices to store certain important information for business continuity purposes, like PINs, passwords, account numbers, etc. This poses a significant risk if this information is compromised. Either the data should be stored in alternative locations for access or, if that is not practical, employ encryption of the data.

Have stated policies on the personal use of company-owned devices, such as whether employees may store personal data such as music, photos, or contacts. Consider policies that do not allow employees to maintain personal data on mobile devices unless they use an application that encrypts confidential data. Whether it is a company-owned or personal device permitted for company use, make it clear that the company is not responsible for theft, loss, retrieval or restoration of personal data or any related implications.

Data Protection

While passwords make it more difficult for unwanted persons to access data on a device, they can, especially if weak, be guessed or "hacked" or they may be circumvented. In these cases, the thief will be able to read all of your data. Encryption replaces useful, understandable data with seemingly meaningless arrangement of useless data. This makes the data more secure as no one can understand it.

To protect the company from data loss in the event a mobile device is lost or stolen, all data on the device and on any removable memory should be encrypted at either the hardware or software level. If the device is not natively encrypted, use manufacturer-provided or third party applications to encrypt the data.[14]

After conducting a review of the U.S. Securities and Exchange Commission's encryption program, the Office of Inspector General made three recommendations to the Commission in its 2010 audit report. Overall, the OIG found the Commission to have a comprehensive encryption program, but found some weaknesses that led to the recommendations. The OIG recommended that the Commission revise its policy and require that "all" portable media be encrypted. It recommended that the Commission eliminate the option for divisions and offices to select whether they will encrypt portable media, such as thumb drives and CD/DVDs. The OIG stated that allowing the user to determine when to encrypt data put the agency at risk and stated that the only way to protect confidential data is through forced encryption of all data. Finally, the OIG recommended that the Commission encrypt all smartphones and PDAs to ensure the protection of confidential and private information on the devices.[15]

Two minimum requirements for mobile devices for data protection should be the remote lock and remote wipe features mentioned above. The remote lock feature allows the company to remotely lock the device to prevent anyone from using it and the remote wipe feature allows the company to remotely delete all data from the device. Combining encryption of removable memory with remote wipe features is critical to protecting sensitive data, as a thief can pull out removable memory from the device before an employee has the opportunity to report the device stolen and the company can issue a remote wipe instruction. Due to the additional risks posed by removable memory, consider restricting its use.

Data Backups

Establish policies for the regular backup of data maintained on mobile devices. Important digital data should never be kept in only one location, so backups should be made to an appropriate location on a regular basis. This is also important from a viewpoint of the recordkeeping requirements. The frequency of backups is dictated by how frequently the information on the device changes, how important the data is, and the implications to productivity if the data is lost. Consider policies that require devices to be backed up to a company server and prohibit backing up of devices to personal computers. Consider requiring backups to be encrypted, especially when permitting personally-owned devices to be backed up to personal computers.

Remote Access

Create polices and internal controls surrounding devices accessing the company network remotely. Polices should ensure that the connection is permitted, access is only granted via authentication, and the connection is confidential.

A firewall is a protective technological wall preventing anyone outside the wall from gaining access to the internal company network. To allow mobile devices, which are outside the company firewall access to the internal company network, a door, called a port, must be opened in the firewall. Similar to homeowners not leaving their front doors unlocked, firewall port openings must be secured to prevent unauthorized access to the network.

Continuing the homeowner analogy, similar to making sure the person using a key to the front door is the proper owner of that key or confirming the identity of the person knocking before opening the door and letting them into the house, a company network needs to authenticate the user of the device that is trying to gain access to the network. The company should have a way of reasonably ensuring that the device is not being used by another unauthorized person, which may be a thief in the case of a lost or stolen device or perhaps even an employee's friend or family member. Furthermore, the company should ensure that the device is not being spoofed, a means of making a connection or device look like the real thing, much like how an impostor tries to fool his/her victims.

Finally, similar to a homeowner not wanting neighbors to overhear their conversations with people standing at their front door, the connection and the data transfer between the mobile device and the network must be secure to maintain data confidentiality and integrity. A communication is considered confidential if only the intended recipient can view the contents of the message. Integrity allows the recipient to detect whether the message was modified by a third party in transit.

To ensure confidentiality of the communication between the mobile device and the company network, the data communication should be encrypted. There are different encryption standards and some are considered more secure than others. Confidentiality can also be ensured through the use of an encrypted tunnel, such as a virtual private network ("VPN"), which creates a secure connection between the device and the company network. Since creating and maintaining this type of connection requires a lot of mathematical calculations, it tends to be resource intensive and negatively affects battery life of mobile devices, thus potentially negatively affecting the user's experience.

Bluetooth Policies

Companies should establish policies that define which devices and employees are permitted to use Bluetooth and whether Bluetooth may be used only for voice communications or also for data transfer. Bluetooth services should be turned off or disabled where not permitted. Additionally, all data traffic transmitted between Bluetooth-enabled devices should be encrypted.

Wi-Fi Policies

Create policies about the use of public networks and train employees on the risks. Employees should always assume that when using a Wi-Fi hot-spot everything they send is readable, interceptable, and usable. Also, putting a device on a public network opens up the device to attack on that network. To protect both the device and the company network, require the use of personal firewalls and end-to-end encryption, such as a VPN. Also, prohibit the use of Wi-Fi for conducting company business if a secure connection cannot be established. Require the use of Wi-Fi Protected Access ("WPA") encryption standards and not Wired Equivalent Privacy ("WEP") encryption, as WEP encryption keys are easily recovered.

Permitted Services and Applications

Firms should establish policies regarding permitted services and disable or remove unnecessary services. Consider the trade-off between the ease of use of a device and the security of the data. For example, a firm may disable laptops from using Wi-Fi and only allow the laptop to connect to the company network from within the network. This will protect the firm from the vulnerabilities of using Wi-Fi, but will limit the use of the laptop when travelling.

IT should maintain a list of approved applications. Only permit the installation of approved applications. Consider requiring through policy or through security controls that only IT can install new applications. As employees request the use of new applications, have a policy for IT to review and amend the approved application list before users can install new applications. Only permit the installation of digitally signed or certificated applications, applications that have been reviewed and approved by the developer. When feasible, enable application features that prevent the installation of applications unless they are digitally signed. Consider policies to

remove any unnecessary applications. When feasible, centrally manage software installation. Consider prohibiting the downloading and installation of applications by the user over a wireless network. Instead, require applications to be installed only through an approved and secure network. For firms permitting the use of personal devices, this would be a very unpopular policy. Also, set policies on whether applications, including third-party applications, on the mobile device can initiate specific types of connections.

Communication Archiving

Finally, set policies on what written communication features may be used. Determine if e-mail, text messaging, PIN to PIN, etc. may be used. The features the firm permits will largely depend on which written communications can be captured and archived in compliance with recordkeeping rules. Establish policies that only permit the use of functions where the data can be captured. If feasible, turn off the features not permitted and centrally control the use of features.

Monitoring and Testing Policies

The final set of policies should include a comprehensive program of monitoring, testing, training, and incident management. The purpose of a monitoring policy is to ensure that security controls are in place, are effective, and are not being by-passed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities. This early identification can help to block the wrongdoing or vulnerability before harm can be done, or at least minimize the potential impact.

Device Testing

The Lincoln Financial and Commonwealth cases demonstrate the need for IT to test that devices in fact are secure rather than relying on the employee to ensure compliance with company policy.[16] Establish policies for IT to regularly test all devices for compliance with company policy. This should not be a one-time test, but should be performed on a regular basis.

Intrusion Detection

Intrusion detection plays an important role in implementing and enforcing a mobile device policy. Due to the number of vulnerability points introduced by the use of mobile devices, some type of assurance is needed that the firm's systems and network are secure from identifiable threats and that systems have not been breached. Intrusion detection systems can provide part of that assurance and fulfill two important functions. They provide feedback as to the effectiveness of access controls. The lack of detected intrusions may be an indication of the robustness of the firm's policies and controls. They also provide a means to detect when the firm's policies and controls have failed and a breach is detected. This allows the firm to quickly take corrective and mitigating action.

Internal Audits/Annual Reviews

Review of mobile device policies and verification of proper implementation of the policies must be incorporated into internal audits and annual reviews. Policies should be reviewed to ensure they remain current with new technology, newly identified vulnerabilities, and company use of mobile devices. Auditors should inspect all devices regularly to verify that policies regarding device access/user authentication, permitted services and applications, permitted data, device settings, device maintenance, and data protection are being adhered to. Testing should also include ensuring that employees have full knowledge and understanding of the risks of using mobile devices and of the firm's policies regarding their use.

Training

Training is critical to the success of mobile device security programs. Firms should train every single individual on their mobile device policies. Training should include awareness training of the types of risks and vulnerabilities that an employee might face and what to do if a device is lost or stolen or a breach is detected. Provide training to all individuals prior to permitting them to use mobile devices for conducting company business. Training should be periodic and kept current for new risks, vulnerabilities, and policies. Consider sending out regular periodic reminders about the risks and policies surrounding the use of mobile devices.

Incident Management

More prolific and broader use of mobile devices to conduct company business increases the risks and potential costs of a data security breach.

Implementing strong mobile device policies, placing limits or controls on how devices may be used or the data or systems they can access, improving user security awareness, and early detection and mitigation of security incidents are some of the actions that firms can take to reduce the risk and drive down the cost of security incidents. In spite of their best efforts to prevent security breaches, firms must adopt policies for dealing with mobile device security incidents in the event they do occur. These policies may be integrated with your general information security or computer incident management policies, but ensure that those broader policies address issues specific to mobile devices. For example, implement policies that cut off the access of the device until the incident is resolved. This would have been an effective means to avert the situation described in the Commonwealth case above.[17]

Management Solutions

While all financial services firms should adopt mobile device policies, not all firms will need or have the means to implement tools to help centrally manage those policies. The larger the firm, the greater the variety of permitted mobile devices, or the greater the data and network access allowed by those devices, the more important it will be for the firm to implement a centralized management solution.

Security controls can be managed and devices can be configured to comply with company security policies from a central location. Mobile Device Management (MDM) software is a tool that uses a management console to control the devices, and one that usually requires each mobile device to have an agent, an application that receives and implements instructions from the MDM. Some devices come with agents already installed; others require the user to go to an "app-store" and download the agent. The MDM server pushes (sends) messages initially and periodically to the mobile device to set and update the device to the desired settings. The use of MDM software can at least partially mitigate the challenges of administering mobile device security program, as it automates many of the configuration, management, and monitoring functions.

When considering MDM software, seek solutions that allow applications to be added and removed from a central management console. Look for security functions that include automatic enrollment and provisioning of configuration profiles. MDM software should be able to detect and block "cracked" devices. Try to find software that can control devices from multiple manufacturers running different versions of many different operating systems on different carrier networks. Look for vendors that are committed to keeping their software current with the rapidly changing technology and have the resources and leadership to remain in the market for a long time.

By maintaining a strong information security program, which should include mobile device security, a firm can prevent or at least mitigate the risks of a security breach.

Seek user-friendly services that do not impede productivity. Raymond James Financial has started to allow their financial advisers to use smartphones in lieu of traditional laptops, but employees have complained that the iPhone software agent they were using to manage security was cumbersome and slowed down the devices.[18] For some ideas on MDM software, look to a Network World article from May, 2011 in which they discuss five different vendors they tested and compared.[19]

Conclusion

Rapidly changing technology, an increasingly mobile work force, and employee desire to use their personal devices, as well as the risks of mobile devices demand that financial services firms implement robust mobile device policies. The need for technological and compliance expertise and the importance of executive decisions on setting policy mandate that compliance, IT, and management collaborate in their development of these policies. Mobile device policies must meet regulatory requirements as well as balance the need for tough security with flexibility of use. Well-designed policies and strong internal controls will serve to protect financial services firms from, or at least mitigate, the burdens and costs associated with the risks of employing both business and personal mobile devices for company business purposes.

ENDNOTES

1 Ellen Messmer, Smartphones and Tablets Create Huge Corporate Security Challenge: Securing Rising Number of Apple iPhone and iPad, Google Android Devices and Others is a Big Corporate Challenge, Network World http://www.networkworld.com/news/2011/061511-smartphones-tablets-security.html (June 15, 2011)

2 U.S. Securities and Exchange Commission, Final Rule: Compliance Programs of Investment Companies and Investment Advisers, Release No. IA-2204 (December 17, 2003)

3 See Regulation S-P, Rule 30a.

4 See Rule 17a-4(b)(4) under the Securities Exchange Act of 1934

5 U.S. Securities and Exchange Commission, Requirements for Brokers or Dealers under the Securities Exchange Act of 1934, Release No. 34-38245 (February 5, 1997)

6 National Conference of State Legislatures, State Security Breach Notification Laws, http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx

7 FINRA Letter of Acceptance, Waiver and Consent, No. 2009020074601, Lincoln Financial Advisors Corporation (February 16, 2011) and FINRA Letter of Acceptance, Waiver and Consent, No. 200901872051, Lincoln Financial Securities (February 16, 2011)

8 U.S. Security and Exchange Commission, In the Matter of Commonwealth Equity Services, LLP d/b/a Commonwealth Financial Network, Administrative Release No. 34-60733 http://www.sec.gov/litigation/admin/2009/34-60733.pdf (September 29, 2009)

9 FINRA Letter of Acceptance, Waiver and Consent, No. 20080152998, D.A. Davidson & Co.

10 Ellen Messmer, Smartphones, Devices Spark IT Security "Mobile Melee": iPhone, iPad, Android, Blackberry devices challenge IT Security Efforts, Network World, http://www.networkworld.com/news/2011/022811-smartphones-security.html (February 28, 2011)

11 U.S. Security and Exchange Commission, Office of Inspector General, Office of Audits, Evaluation of the SEC Encryption Program, Report No. 476 (March 26, 2010)

12 National Institute of Standards and Technology, U.S. Department of Commerce, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): Recommendations of the National Institute of Standards and Technology, Special Publication No. 800-122 (Erika McCallister, Tim Grance, and Karen Scarfone, April 2010)

13 Network World, June 15, 2011

14 Apple, Inc., iPhone and iPad in Business: Deployment Scenarios, http://images.apple.com/iphone/business/docs/iOS_Business.pdf (October 2011)

15 Evaluation of the SEC Encryption Program. 5

16 In the Matter of Commonwealth Equity Services, 2,4; and LAWC Lincoln Financial Advisors, 3; LAWC Lincoln Financial Securities, 2,5

17 In the Matter of Commonwealth Equity Services, 1

18 Network World, February 28, 2011

19 Tom Henderson and Brendan Allen, How to Protect Smartphones and Tablets: New Tools Tame Apple iOS, Android, Blackberry devices and more, Network World, http://www.networkworld.com/reveiws/2011/052311-mobile-device-management-test.html (May 23, 2011)