Contents

This white paper addresses the risks associated with the relatively new phenomena surrounding the introduction of corporate-owned data on Portable Devices, currently known by buzzwords such as mobile computing, mobile devices, mobile technology, etc. As the information security community scrambles to understand methods of protecting data on both employee-owned mobile devices, known as BYOD (bring your own device), as well as company issued devices, the cost savings of "going green" with iPads, Android Tablets, and Smartphones has put the cart before the horse in many organizations. To properly modify the IT Policy of a company, in order to address this phenomenon, is no easy task.

This white paper accompanies our premier offering of our **Mobile Devices Security Kit**; a new offering for Infotex.

A convergence of needs

The creation of IT policy and strategy governing the use of mobile devices, whether owned by the company or not, revisits every need ever raised in the effort to create a security policy: the need to start with a risk assessment; the need to ensure appropriate alignment between policy, procedure, and technical configuration; the need to shop a sample IT policy through senior management and non-technical users; the need to integrate audit plans with deployment; and the need to inform employees of their rights and responsibilities via appropriate IT security policy; all these needs come together when addressing security in the mobile environment. This convergence of needs twists the thoughtful information security manager to the point where the question, "What is a security policy, anyway?" returns us to the debate about how one should divide documentation into policies, procedures, and standards.

Definition

Even the decision on how to name control documents became an issue. We ended up choosing Portable Device instead of mobile device so as to not exclude traditional portable devices such as laptops and tablet PCs. To address BYOD and mobile devices in general, we wanted to create a set of documents that covers all devices, whether owned by the Bank or not, that access Bank assets from outside of the branch. Making our task more daunting was our own need to ensure that a security policy template would easily scale from a small bank to a large bank, while translating to different industries, especially including industries with HIPAA, PCI, and SOX IT Security Policy requirements. Having released our original "cell phone policy" in 2003, we wanted to incorporate all devices attaching to the network from outside of the branch. This may stem from our work on our upcoming Branchless Banking Kit, but it seemed to make a lot of sense with our beta-test banks.

Definition of Portable Device

Name of Financial Institution defines portable devices as "any self-contained device that can transfer and store data which has the ability to be routinely removed from the network and carried outside of the organization, whether owned by the financial institution or not." The following is a non-inclusive list of typical portable devices:

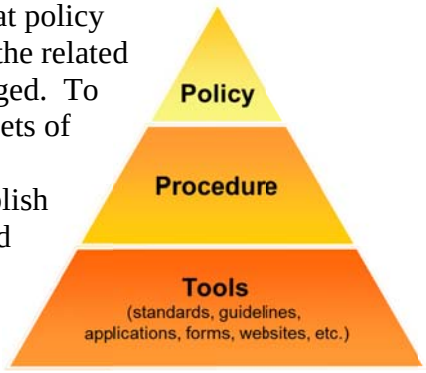
- Laptops
- iPads or other Tablet PCs (such as the Motorola Xoom)
- Smart Phones (such as iPhones, Droids, etc.)
- Regular Cell Phones with Storage Capabilities (such as Blackberries, Treos, etc.)
- Digital Cameras
- iPods and/or MP3 Players

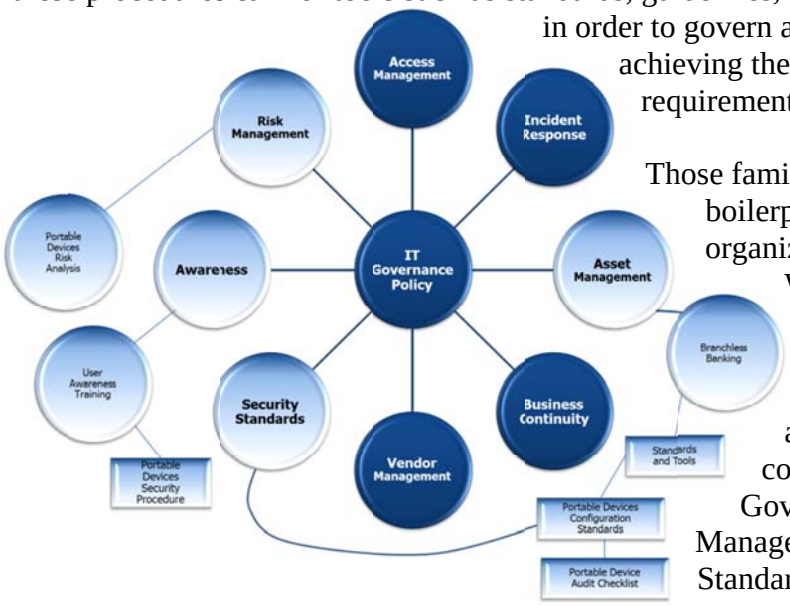
This definition does NOT intend to include "portable electronic media" such as CD's, DVD's, USB Drives, or SD-Flash Cards, though such media may be used in portable devices. The Acceptable Use Policy governs the use of electronic media.

Thus, rather than focusing solely on Smartphones like the iPhone and Android; or Tablets such as the iPad or Playbook or Galaxy; we expanded the scope of this kit to also address laptops, cameras, and any future device that would fit the definition of what we are calling "the portable device," as articulated by our policy template in the box to the right.

Policies, Procedures, Standards, and Tools

Before one modifies the IT policy of a company, they must understand how that policy relates to all other documentation in the bank. And they must understand that the related documents merely describe living and breathing processes that may have changed. To help with this, most organizations now organize their compliance response in sets of "programs" that each includes three primary levels of documents. Policies are documents approved by ownership (usually the board of directors) which establish objectives, requirements, authorities, and responsibilities. Policies are enforced by employees following a set of documented procedures that users follow, and these procedures call for tools such as standards, guidelines, and applications in order to govern a process for achieving the objectives and requirements of the policy.





Those familiar with Infotex have probably adopted our boilerplates and templates within the context of your organization's existing IT Governance Program. Whereas programs are a collection of policies, procedures, and tools used to govern a particular process, kits cross the boundaries of a program. At Infotex, we call our Mobile Security Policy Kit a kit instead of a program because the documents it contains fall into more than one area of a typical IT Governance Program, ranging in diversity from Risk Management to User Awareness to Technical Security Standards.

You'll notice we did NOT use the name "mobile devices" in our procedures documents. We selected the term "portable devices" after much debate with "mobile devices" and "branchless banking devices" as close alternatives. The term "portable devices" seemed to lend itself better to cover all current and hopefully all future types of information assets that would have the following characteristics:

A. Be used by user-level employees.
B. Be hardware.
C. Be turned on outside of a branch or office.
D. Have the potential of hosting sensitive information.
E. Have the potential of accessing Bank assets.

Three critical needs must be addressed by our response to mobile device risk:

1. Development of a User-level Policy (we call it the Portable Devices Security Procedure) signed by BYOD or Issued Device users.
2. The documentation of technical configuration standards (we call it the Portable Devices Configuration Standards) so that technical controls are known not only by technical staff, but auditors, examiners, and managers.

3. Some method of auditing portable devices (we propose a Portable Devices Audit Checklist) so that users can not only be held accountable for non-technical configuration standards, but they also can be trained on how to ensure those standards are being enforced.

Thus our kit includes a user-level policy document that calls itself a procedure (not only so that it does not have to be approved by the board, but also because it does not apply to ALL users, but only a small subset of users). Interestingly, many banks will require their board members to sign-off on the procedure as a user, as board meetings begin to leverage mobile technology such as board portals and iPads.

The Mobile Devices Security Kit

As a whole, our kit addresses all mobile wireless security issues. It can scale to smaller banks simply wanting to take advantage of resources already available (such as Exchange ActiveSync); but it also scales to organizations looking to leverage some of the sophistications of Mobile Device Management applications (MDM.) We start where the FFIEC wants us to start— with a mobile risk assessment—and then proceed with real-world device security decisions in the documents we use to help establish guidance. The risk assessment, of course, includes proposed declared controls that are covered by the mobile policy and procedure documents, as well as an asset inventory. The remaining documents simply address the risk found in the risk assessment, including inserts to be added to your existing Acceptable Use Policy and high-level IT Governance policy, as well as the Portable Devices Security Procedure (which some may rename Mobile Security Policy), that also includes an agreement sign-off form that will establish user rights, and warn users of what exactly will happen due to some of the more intrusion security policies such as the potential remote wipe of their handheld device.

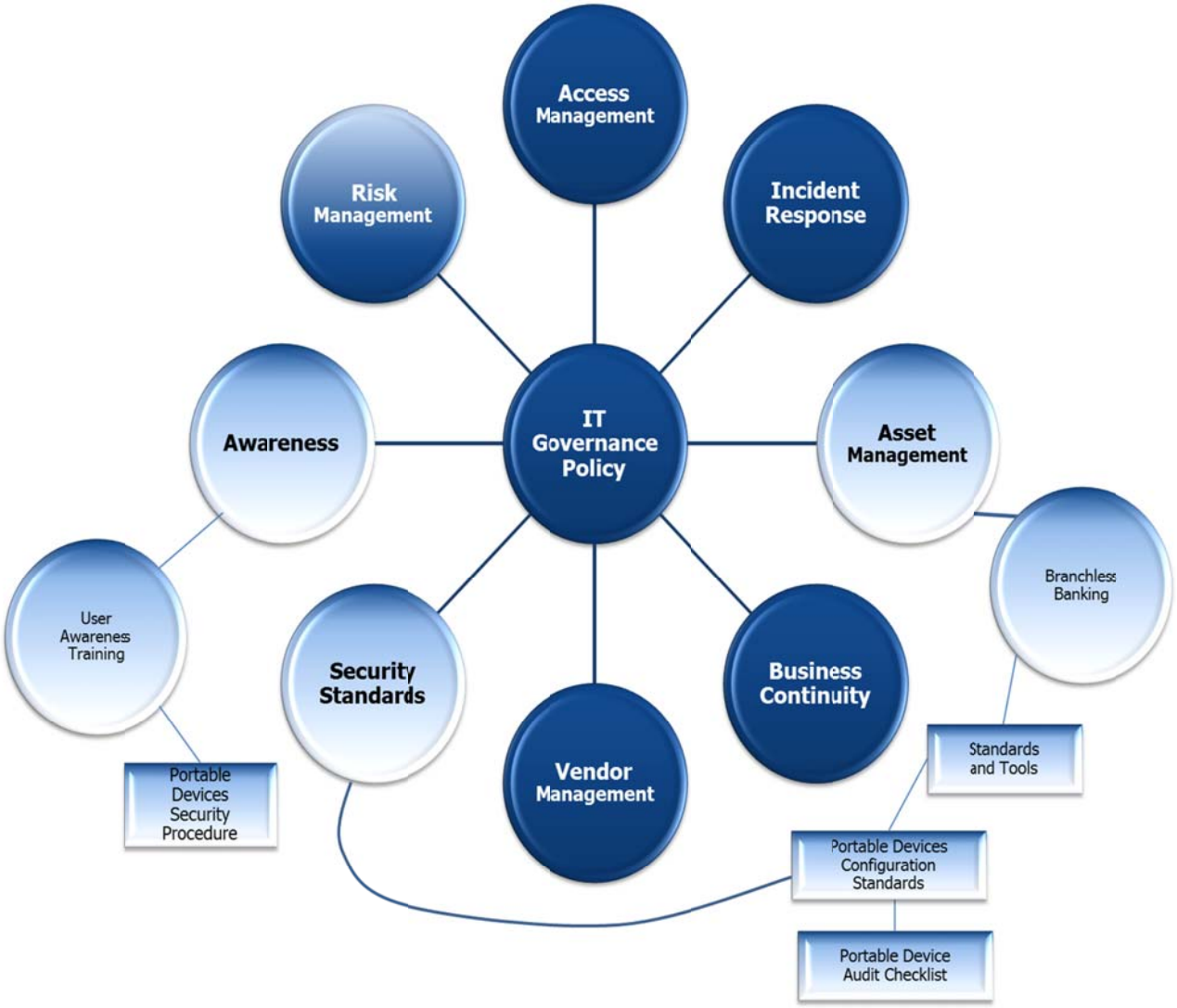
- **Portable Devices Risk Assessment:** The FFIEC is clear about the need to conduct risk assessments focused on the deployment of new technologies. This document is an asset-based drill-down risk assessment that can be used to establish inherent and residual risk on vulnerabilities to smartphones (iPhones, Android Phones, Blackberries), tablets (iPads, Galaxy's, Playbooks, etc.), and laptops. It includes a handy asset inventory.
- **Portable Devices Security Procedure:** This user-level document governs how users are to use, secure, maintain, and return a portable device. It covers both authorized (BYOD . . . employee-owned) devices as well as issued (bank-owned) devices. The required controls it establishes are worded as a trade-off: "if you enforce these controls you get to put bank data on your phone."
- **Agreement to comply with Portable Devices Security Procedure:** This agreement is very important so that employees understand their obligations, responsibilities, rights, and vulnerabilities. The warnings in this agreement are paramount for a solid risk management approach, for warning employees of the pitfalls of remote wipe (you will lose your pictures and music), and also to smooth over some of the more unpopular inconveniences of the program (such as the right to audit).
- **Agenda for Configuration Standards Meeting:** This document is intended to help your technical team walk through the issues that must be understood before implementing BYOD and MDM (mobile device management) controls. It includes documentation such as how to tell if a device has been jailbroken as well as establishes discussion topics such as Apple Configurator and Exchange ActiveSync.
- **Portable Devices Configuration Standards:** This document establishes all the technical security standards that must be met to properly enforce the modified Acceptable Use Policy and high-level IT governance policy as well as, of course, the Portable Devices Security Procedure. Again, it scales from a "poor-man's approach" to technical control enforcement through the use of sophisticated Mobile Device Management applications (MDM).

- **Portable Devices Audit Checklist:** This three-part checklist allows your technical team (or whomever is identified in your policy statement) to audit both BYOD devices and bank-issued devices. It includes an asset inventory as well as a checklist for smartphones, tablet pc's, and laptops.

Policy or Procedure?

Many banks would consider the Portable Devices Security Procedure to be a user-level policy that, unlike the Acceptable Use Policy, is only applicable to certain employees (those authorized as per the procedure). The Portable Devices Security Standards document is a technical standards document that may or may not be a formal part of your Information Technology Governance Program. It is meant primarily for those involved in configuring and auditing the configuration of portable devices. However, it also covers portable electronic media, whereas the user-level Portable Devices Security Procedure only covers portable devices. Portable electronic media (such as flash drives, CD-ROMs, DVDs, etc.) is usually covered, at the user-level, by the Acceptable Use Policy (since all employees have the potential of using electronic portable media).

For those institutions who have already adopted many of our templates, the following diagram can help you fit the Portable Devices Kit into the overall IT Governance Program:



Considerations

We believe that a good strategy to protect Bank information assets from the use of "portable devices" needs to consider:

1) Both employee-owned (Bring Your Own Device [BYOD]) and Bank-owned devices.
2) All devices that access Bank assets from outside the branch.
3) The entire device lifecycle (introduction, management, retirement).
4) Not just smart phones and tablets, but also laptops, cameras, and the next "widget."

Conclusion

We would be happy to answer any questions that you may have about the **Mobile Devices Security Kit** that we have created. We'd be open to helping you customize it to your bank.

Sincerely,

Dan Hadaway and the Infotex Team