

▶ Mobile Security

Small Packages, Big Risk

Preventing data leakage through your agency's system ports requires a smart plan of action combined with vigilant monitoring of your users' mobile devices. **By John Jefferies**

Tiny computing and storage devices can stow the equivalent of millions of pages of data. But they also offer hostile agents an easily concealable package for carting off sensitive or classified government information.

Lost or stolen flash drives containing everything from citizens' private data to military secrets and plans for the joint strike fighter have turned up in rental cars, gas stations — even a bazaar in Afghanistan. Whether measured in national security or legal costs and remediation for affected individuals (or in damage to the reputation of an agency from public disclosure), data breaches can have devastating consequences.

Managing these risks without nullifying the significant productivity and efficiency benefits of smartphones, personal digital assistants, flash drives and other mobile devices demands a delicate balancing act by the government's IT departments. Here is a road map of best practices — which address encrypting data on mobile devices, controlling access that devices have to government systems and managing devices centrally — for organizations grappling with this challenge.

At the Minimum: Encrypt Mobile Data

No organization can afford to leave sensitive data in an unprotected state on devices that can easily fall into the wrong hands. Strong encryption provides the best first defense against loss or theft. According to the National Institute of Standards and Technology, it would take approximately 149 trillion years to crack a 128-bit Advanced Encryption Standard key.

Nonetheless, when deploying encrypted devices to employees, make sure they use the recommended mode of AES encryption. Electronic codebook is the easiest to implement but does not provide adequate confidentiality for files. Cipher-block chaining provides greater security, but because it is harder for manufacturers to implement in hardware-based encryption — especially when using fast flash memory — it is not often used.

The encryption solution must be certified as compliant with Federal Information Processing Standard 140-2 at Level 2 or above. NIST certification ensures that device designs and encryption methods have been implemented and performed correctly.

Despite the strength of FIPS-certified AES encryption, it is only as strong as its weakest link, which happens to be each user password. A number of password-guessing software and hardware tools let hackers decode a user's password by hammering away at a device with millions of guesses per second.

Encryption solutions that store passwords and encryption keys in hardware can prevent brute-force attacks, especially since software-based solutions allow hackers to rewind the counters designed to limit the number of times an incorrect password can be entered. **The only truly reliable encryption solutions on portable devices are hardware-based.**

Hardware-based encryption can also protect against cold-boot attacks, where hackers gain access to the encryption keys from RAM memory because keys remain in memory for a time when the device is asleep and after it has been powered down.

Users also represent a threat. Some write down passwords and carry lists with them — often with their mobile devices. Still others may have valid passwords yet represent a malicious insider threat. And some data on a smartphone is available without a password.

MIKE KEMP/UPITER IMAGES

“By combining managed hardware encryption with port control, agencies can virtually dial back the risk of data loss and leakage via mobile devices.” — JOHN JEFFERIES



Encryption alone is not enough; agencies need to use encryption within the framework of a centrally managed security strategy, including the ability to remotely disable or deny access to compromised devices, or wipe them clean.

The Central Issue: Manage Mobile Devices Centrally

Convenience: It makes smartphones, USB flash drives and other mobile devices attractive to users. An estimated 300 million USB drives are in use worldwide. There are so many devices in the hands of users that on any given day, many organizations remain unaware of how many devices connect to their networks, or from where. With little control and knowledge of how devices are used or their security posture, these legions of mobile users represent a significant security risk.

Some organizations have already taken steps to centrally manage end-point data protection for their desktop and notebook PCs. The next logical step is to take the same approach for mobile devices. This means going beyond standalone encryption to implement capabilities for tracking use and enforcing security policies remotely, including the ability to lock a device after a number of incorrect attempts to guess a password or to destroy data if a user reports a device lost or stolen.

By deploying devices within an enterprise management framework, agencies can implement policies that define acceptable use, such as remote access, authentication, device storage and encryption.

Pulling the Plug: Control Ports

Besides managing devices, organizations should also consider controlling ports to which they connect. But gluing USB ports shut or otherwise disabling them denies employees the productivity benefits gained by using mobile USB devices. This approach is not viable because these ports are necessary for key peripheral devices, including keyboards, mice and printers.

Because employees need access to these

ports to do their jobs, IT should employ flexible approaches, such as whitelists that let only authorized devices connect. A number of available device control applications let administrators establish whitelists so granular they can specify individual device serial numbers.

By combining managed hardware encryption with port control, agencies can virtually dial back the risk of data loss and leakage via mobile devices.

Remote Control: Establish Secure Remote Access

For many civilian and military applications, IT administrators must define policies for remote access, including acceptable network connection methods and authentication policies that define who receives what type of access and to what data. Remote devices often become part of the solution by incorporating some form of two-factor authentication.

Digital certificates and secure, one-time password generators, such as RSA SecurID authenticators, extend secure authentication beyond passwords. Eliminating the need for a physical token or additional device by having two-factor authentication built into an encrypted USB drive can improve security because the user cannot access credentials until after securely logging onto the device.

THREE MORE STEPS

- Use hardware encryption and device control to encrypt all portable devices and prevent users from attaching unauthorized mobile devices to computers. These measures protect government networks that contain sensitive data from careless or malicious users of the devices.
- Set policies for remote deactivation of devices so that, should a device be lost or stolen, IT can prevent unauthorized access to the data.
- Let employees use only authorized devices that IT has programmed with common policy controls.

This approach also reduces costs while streamlining both administration and the end-user experience.

Known Variables: Educate Employees About Risks

Studies by the Ponemon Institute have found that when faced with getting their job done or following security policies, 95 percent of employees choose the former. Consequently, they often carry sensitive data on these devices against policy or use them on insecure networks where bots, keyloggers and pharming code can load surreptitiously and then allow access to secure government networks.

Employees need to understand the importance of the security measures set by IT organizations. Unless they fully understand the magnitude of the threat and importance of reducing risks, they will view policies as barriers to productivity.

With a securely managed infrastructure of mobile devices, employees could, for example, carry a virtual PC desktop on an encrypted flash drive. In the event of a fire, flood, terrorist attack or other disaster, workers could set up a fully functional replica of their office environment on any computer, including access to all their data and applications. Two-factor authentication built into the device would further ensure quick and easy network access.

By following best practices, federal organizations can protect themselves from the risk of data loss and leakage, enabling flexibility and mobility — and ensuring continuity of operations. **FT**

John Jefferies is vice president of marketing at IronKey.

Reprinted from *FedTech Magazine*.
IronKey, Inc.
5150 El Camino Real, Suite C31
Los Altos, CA 94022 USA
T 650 492 4055
sales@ironkey.com www.ironkey.com

