NASCIO
Representing Chief Information Officers of the States

JULY 2009

NASCIO Staff Contact:
Charles Robb
NASCIO Issues Coordinator
crobb@AMRms.com

Security at the Edge — Protecting Mobile Computing Devices

Amazing Technology, More Powerful Mobile Computing, Significant Risk

Use of mobile computing devices within the state government workplace is expanding at an ever-increasing rate. Work that has long been performed outside the confines of state offices is now supported by handheld computers and in-car laptops that assist police, emergency management, environmental and agricultural inspection, and fish and wildlife monitoring functions, just to name a few. Performing the same functions without such tools is hard to imagine. State business that once had to stop while employees were away from their desks now continues through the use of smartphones that provide an uninterrupted stream of voice, data, and email communication, thereby reducing business latency and enhancing service delivery. For the once office-bound workforce, mobile devices support green, environmentally-friendly, and cost-reducing telecommuting, as work is effectively performed from home offices. In short, today's business drivers compel state governments to take greater and greater advantage of mobile computing tools.

While mobile devices provide significant productivity benefits, they also pose new risks to an organization's security. Enhancements in their power and their storage capacities make their physical loss much more damaging to the organization. As importantly, they become increasingly attractive to profit-motivated cyber criminals, who view them as both valuable and easy targets, especially during an economic downturn. The sheer increase in their numbers, combined with their small size, make them extremely vulnerable to simple loss or theft – as the National Institute of Standards and Technology

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
Email: NASCIO@AMRms.com

(NIST) notes, their propensity to become physically separated from the user is extreme.[1] Yet physical loss is just one of the threat vectors posed by their use.

Ponemon Institute conducted research sponsored by Dell last year that estimates that more than twelve hundred laptops are lost at U.S. airports per week. [2]

Making a tenuous situation worse is the way mobile devices have commonly entered the workplace, often through unauthorized adoption or informal requests by end-users or individual lines of business. This diverges from the centralized, policy-driven IT infrastructure management model, and has led to significant problems as users argue with IT over whether use of the devices is valid in the first place, the way in which they can or cannot be connected with the secured network infrastructure, and the way in which they may be used for a combination of business and non-business purposes. Unless CIOs and CISOs take strong action to mitigate the problems associated with mobile devices, they represent a significant and growing vulnerability.

Ponemon Institute research suggests that over 42% of all U.S. data breaches stem from lost or stolen laptops.

Why This is Important or "The Facts Don't Lie"

There is compelling evidence that mobile devices pose one of the fast growing areas of security concern. Since January 2008, Privacy Rights International's published Chronology of Data Breaches documents that ninety-one (91) of the 444 data breaches reported (20%) resulted from mobile device losses – lost laptops, notebook computers, PDAs, portable drives, USB drives, CDs, flash cards, SD cards, and diskettes. (Yes, they still make diskettes, and governments, of course, still use them.) During that time period, over 2.75 million records on individuals were lost, though the number is smaller for breaches for public agencies (federal, state, and local governments, K-12 and postsecondary public institutions). The number of reported devices lost from state agencies is smaller, but state agencies lost 1.2 million records.

Ponemon Institute research suggests that over 42% of all U.S. data breaches (all sectors, public and private), stem from lost or stolen laptops. They also estimate that the average cost for each breach was nearly $50,000.[3]

News Item – A Canadian Example 300K Patient Files on Stolen Laptops

Alberta's privacy commissioner has launched an investigation into the theft of two laptops from a University of Alberta lab, reports CBC News. The computers, taken from Alberta Health's Provincial Lab Information Technology room, held personal information on 300,000 people, including names, birth dates, personal health numbers and lab reports, the report states. Alberta Health officials said in a press release that the information is behind several passwords, but that patients should monitor for identity theft. Privacy Commissioner Frank Work expressed surprise that the laptops were not encrypted. "The standard in Alberta...is encryption...," Work said. "***How can the public have faith in public bodies if they can't [secure] personal information?***" 6/25/2009 IAPP Dashboard (Emphasis added)

Needless to say, state governments cannot afford either the dollar losses associated with such breaches, or the loss of credibility and public trust associated with the more tangible losses.

Definitions

Mobile Devices: NIST defines mobile devices as portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain non-volatile memory) or portable computing and communications device with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones). [From NIST 800-53]

Data Breach: A breach is a loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an authorized purpose have access or potential access to personally identifiable information (PII) in usable form, whether physical or electronic.[4]

What Are the Issues?

NASCIO publications have addressed mobile device security in the past.[5] The September 2008 brief, *Protecting the Realm*, noted that many data breaches have resulted from lost or stolen mobile devices, and that the encryption of information both at rest and in transit has become one way that states and other entities have addressed data protection concerns with mobile devices.

A more detailed list of issues associated with mobile device loss includes:

- The nature of the information/data may be highly sensitive.
- The nature of the information/data on the device may be unknown.
- The information/data may not be backed up, or if backed-up, may not be backed up on enterprise servers.
- The information/data may include non-business related material which is inappropriate for maintenance on a state-owned asset.
- The information/data may have resided on a personal device owned by the end-user, rather an on a state-owned asset.
- Encryption may not be employed or, if employed, may not meet enterprise standards.
- Password protection or other authorization/access control mechanisms may not be in place, or again may not meet enterprise standards.
- The device may not be subject to remote wiping.
- The device may or may not be on an inventory, or the inventory may not be integrated with that of other IT assets.
- Users may be unaware of appropriate use and security requirements associated with mobile devices. They may not understand special responsibilities associated with their use of mobile devices, nor where their responsibility ends and IT's begins.
- Use of the device over WiFi networks may be insecure. Gartner notes that most end-users employ WiFi in public mode, without firewalls, authentication or encryption.[6] By doing so, they risk inbound network service attacks, over-the-air data capture, as well as phishing and spoofing attacks.

A salient take-away from this list is that some or all of these conditions are present or even prevalent in government programs. This stems from the fact that mobile device technology sometimes advances faster than enterprises can act to control it — for many, the mobile device has become the computing platform of choice — the default, not just a second device. The distributed and ad hoc nature of the mobile environment makes control and compliance significantly more difficult.

For many, the mobile device has become the computing platform of choice.

Following a serious data breach in Ohio in 2007 that resulted in the loss of sensitive information relating to 1.2 million citizens and businesses, the state responded by investing in an endpoint encryption software solution that now protects over 70,000 mobile devices used by the state's employees.

The estimated cost of the Ohio data breach was over $2 million. The software solution implemented there cost approximately $1.1 million. While every state CIO and CISO would rather pay before the breach, competition in states for this level of funding is extremely intense in the current fiscal environment.[7]

End-users may be comfortable mixing work-related email, documents, and data with their own personal correspondence, photographs, and music, but governments cannot afford to take that risk.

Enterprises need to manage mobile devices with the same care as desktops, but are sometimes stuck with an approach left over from the early years of "personal" computing in the enterprise, when PCs were novel and adoption was driven by end-users or individual business units. It is also true that enterprises and lines of business somehow continue to undervalue the data and information they maintain, being still at a relatively early stage of evolving into 21st century governments.

Fundamentally, mobile devices are being used to maintain assets that must be protected. Where adequate resources are available, the trend in state government is to implement better policies and controls, along with adequate hardware and software solutions, to better control both the data and the mobile devices themselves. Integration of those mobile device policies and controls with the larger security and management frameworks is also the norm in more advanced security programs.

In opposition to that trend, however, is the increased power and adoption of consumer-based tools that have evolved into robust computing platforms that connect to the network at ever higher speeds, as G3 gives way to G4. These create significant pressure from the state workforce for IT to provide comparable tools and functionalities in the workplace, or failing that, to allow end-users to connect devices they acquire for personal use to state-owned resources. It is frequently lost on end-users that built-in security capabilities present in their handheld devices, which might be valuable for personal use if properly configured, are still completely inadequate for the protection of government data. Similarly, it may be lost on the manufacturers of such devices that state enterprises have broader and deeper requirements for protecting the integrity and confidentiality of state information. End-users may be comfortable mixing work-related email, documents, and data with their own personal correspondence, photographs, and music, but governments cannot afford to take that risk. FOIA/open records requests for items on such devices will be both difficult and potentially embarrassing for CIOs and other state officials to fulfill.

With the reality of mobile device productivity enhancement, convenience, and computing power in ever-smaller form factors, CIOs and CISOs face a new reality they have to come to grips with.

Where are States in Implementing Security Policy and Practices to Protect Mobile Devices?

Many state IT organizations (Delaware, Michigan, North Carolina, Ohio, and Tennessee, among others) have made strong efforts to mitigate the risk of lost mobile devices through the adoption of across-the-board encryption of all mobile devices. Typically, these efforts are piloted in agencies or cabinets with a preponderance of sensitive data, which creates a crucial business driver for stronger data protection. Pilots are then expanded to encompass the remainder of state agencies. Many states are taking this approach toward encryption and are at various stages in the process of execution. Other states, likely as a means of controlling costs, have taken a more selective approach and target the most sensitive data.

A less positive business driver is that breaches have occurred in some states, which has led their IT organizations and resource allocators to invest in the acquisition of tools to better control mobile devices. Here a key point must be made – the risks associated with mobile device use are generally well understood by state CIOs and the CISOs and security personnel who support them. In general, where the latter have been successful in communicating the degree of risk to resource allocators, sufficient support has been provided to enable development of policies, standards, and procedures and the acquisition of hardware and software solutions.

The progress of other states has been somewhat slower, because the risk sometimes appears abstract if breaches have not occurred, and because significant dollar investments are necessary to acquire and implement technical solutions that encrypt and otherwise protect the devices. The current fiscal environment in states obviously poses significant challenges. Absent adequate resources, CIOs may be forced to defer needed investments. CIOs can mitigate the risk to a degree through policies and end-user education, but there are ultimately limits to the effectiveness of such measures. Mobile device theft or loss is a ticking bomb that will ultimately go off unless other solutions are implemented.

CIOs should be aware that the federal government's software procurement program SmartBUY offers federal agencies significant discounts on commonly used, off-the-shelf encryption products that have met Federal Information Processing Standards (FIPS) cryptographic requirements for data at rest. The Multi State Information Sharing and Analysis Center (MS-ISAC) has made efforts to publicize this program and has urged states to make use of SmartBUY to make these types of products more affordable and thus more prevalent in state security programs and initiatives.

Additionally, CIOs, recognizing that their obligations extend beyond protection of the data to the protection of the hardware assets themselves, should monitor the growing use of software that acts post-theft to notify owners when their devices are reconnecting to the network. Available through a variety of vendors, these tools are becoming more and more affordable and are already used effectively in a variety of Federal agencies and university programs.

On the whole, despite growing pressures from end-users, state governments have resisted the formal or broad scale adoption of mobile devices into the workplace unless they come with supporting technologies that enable their central management and configuration. This may mean the most advanced smart phone available on the street cannot be authorized for use throughout the state workforce. However, as accompanying and appropriate security technologies are packaged with such products, they may be incorporated into wider use. CIOs and CISOs must here perform a balancing act that supports business needs adequately without accepting inappropriate levels of risk. End-users must understand that while corporate decisions regarding appropriate hardware may not always equip them with the latest and greatest mobile devices, they must live with those decisions.

Where Standards Fit

A solution directed solely at encrypting mobile devices is obviously beneficial, but both Federal guidance and best practice advice and recommendations from the International Standards Organization and others recommend that states take an approach that integrates mobile device security within the larger security frameworks established by IT programs. The component parts of this approach include policy, standards, and procedure development and execution, end-user education, and the implementation of a range of policy driven controls accompanied by use of hardware and software tools.

States that have adopted security standards frameworks, as NASCIO recommended in ***Desperately Seeking Security Frameworks – A Roadmap for State CIOs*** (March 2009)**,** have an advantage. Those frameworks already incorporate mobile device management, and the extension of controls over the environment of mobile devices is relatively straightforward, albeit labor- and cost-intensive.

States that have adopted security standards frameworks have an advantage.

North Carolina, for example, cites ISO 27002 in the following section of their IT security manual:[8]

050408 Day-to-Day Use of Laptop/Portable Computers
Purpose: To promote the secure day-to-day use of laptop/portable computers.

STANDARD
Personnel who use an agency laptop/portable computer shall ensure that the laptop/portable computer and the information it contains are suitably protected at all times.
Agencies shall require that laptops and other State-issued mobile electronic devices have:

- Full disk encryption
- Locks.
- Regular backups.
- Current antivirus software.
- Firewalls configured to comply with State and agency policies.

Where technically possible, agencies shall require that other mobile electronic devices used for conducting the state's business comply with the same standards as laptops. Where full disk encryption is not technically possible, mobile electronic devices shall have other protection mechanisms such as BIOS password or PIN access.

Agencies shall periodically audit these devices to ensure compliance with these requirements.

Comprehensive security guidance of direct help to states in executing mobile device security programs may be found in the following publications:

NIST Special Publication 800-124, Guidelines on Cell Phone and PDA Security (2008) -
http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

NIST Special Publication 800-114, User's Guide to Securing External Devices for Telework and Remote Access (2007) –
http://csrc.nist.gov/publications/drafts/800-46-version2/Draft-SP800-46v2.pdf

NIST Special Publication 800-46 Revision 1, Guide to Enterprise Telework and Remote Access Security (2009) -
http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf

Expect Bad Things to Happen – Take Action Now

CIOs must deal with reality when it comes to mobile devices – the productivity enhancements they provide, their convenience, and the computing power they offer in a very small size, mean their presence in the workplace will continue to grow. The distributed, ad hoc nature of the mobile environment, however, makes mobile device control and compliance more difficult even while it is absolutely necessary.

State IT organizations must respond to this challenge as part of their larger enterprise security architectures by extending the latter's component elements (network access controls, patch management, intrusion prevention systems, firewalls, access management, encryption requirements, etc.,) to the domains of mobile and smart wireless devices.

As part of that security framework extension, CIOs and CISOs must –

- Establish expectations for use of state and non-state owned mobile tools, articulating appropriate use scenarios consistent with business requirements, the sensitivity of the data to be maintained on the device, and legal requirements relating to the management of government records and data. Guidelines should indicate what information/data/records can be maintained outside the secured corporate environment and which data must be encrypted.[9]

- Incorporate mobile device management into the larger IT asset management frameworks administered by state IT programs. Where ownership and management are distributed outside the central IT organization, clear roles, responsibilities, and authorities must be established.

- Ensure management of mobile devices and the information maintained on them through their full life-cycles, backing up, transferring, and maintaining data/records/information consistent with established retention policies and guidance, and sanitizing and disposing of physical devices using appropriate controls and procedures.

- Clearly establish end-user responsibilities in the reporting of data breaches or loss of devices, as well as the responsibility of the IT agency.

- Anticipate that devices will be physically lost and encrypt the data stored on them to the broadest extent possible.

- Require authentication with strength appropriate to the sensitivity of the data maintained on the mobile device.

- Ensure security is a key purchasing consideration for all mobile and wireless technology and services, and a component of all RFPs relating to their acquisition.[10]

The network boundaries that CIOs and their organizations have secured in the past have effectively been extended and will continue to evolve as broadband and wireless technologies grow more and more powerful and ubiquitous. Regardless of that, the data flowing within that expanded environment must be secured and protected to the same degree it was when technologies were less complicated.

While challenging, the tools for improving mobile device security are available and must be brought into more widespread use. Taking the steps outlined above will enable state IT organizations to significantly reduce the likelihood of data loss and breaches that have often accompanied expanded use of mobile devices.

Appendix A: Endnotes

[1] http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_devices/PP-UNIsecFramework-fin.pdf

[2] Airport Insecurity: The Case of Lost & Missing Laptops. Ponemon Institute, June 30, 2008.

[3] The Business Impact of Data Breach, Ponemon Institute, May 15, 2007

[4] From www.census.gov/privacy/docs/databreachpolicyimplementationguide.pdf

[5] "The Year of Working Dangerously—Parts I and II: The Privacy Implications of Wireless in the State Government Workplace," August and September 2005

"Insider Security Threats: State CIOs Take Action Now!", April 2007

"Protecting the Realm", September 2008

[6] "Best Practices in Wireless and Mobile Security: Planning for 2009," Gartner, 2008, p. 2.

[7] See http://www.privacy.ohio.gov/government/

[8] http://www.scio.state.nc.us/documents/docs_Active/Statewide%20Information%20Security%20Manual/Chapter5.pdf

[9] "Use Managed Diversity to Support Mobile Devices," Gartner, 2008, p. 9.

[10] "Best Practices in Wireless and Mobile Security: Planning for 2009," Gartner, 2008, p. 1.