Mobile threats: Real but largely preventable

The number and variety of threats to mobile devices and the data they access will never disappear—and in fact, new threats will continue to arise. But with the right tools and planning, most of these threats can be thwarted before they harm an agency, its data or its users. Here are some of the biggest threats to watch out for:

Malware and Spyware: According to Juniper's latest Mobile Threat Center research, the number of malware programs threatening mobile users grew by more than 600 percent in 2012 over the previous year. That number covers many types of threats, including:

Trojans: Code inserted into applications or executable files that are downloaded to the device. Once executed by the user, Trojans can steal data and take over device resources.

Worms: These programs, which can lead users to take actions that cause harm, create similar or exact copies of itself that can reproduce itself to other devices.

Ransomware: This fairly recent type of malware can either be installed when a user visits a malicious website or when a user opens a malicious email attachment, link or instant message. In its 2014 Predictions Report, McAfee said it expects ransomware to proliferate on mobile devices.

Spyware: When installed on a mobile device, spyware can collect data about a user's web browsing history, personal contacts and locations visited and send that data back to the hacker's location.

Data leakage: If mobile devices aren't subject to stringent controls, it's not only possible that sensitive data will get into the wrong hands—it's likely. And it's all too common. A Juniper research report on mobile security found that more than 80 percent of enterprise and consumer devices are unprotected and at risk of data leakage.

Here are a few examples of how this could happen:

- A government employee sends an email attachment to an external partner over an unsecured WiFi network.
- A government employee stores work files in his own personal Dropbox in the cloud, which can be accessed by anyone he invites in.
- A government employee downloads a non work-related app onto the mobile device she uses for work.

Data device loss/theft: When employee loses a mobile device, it is costly. Beyond the hardware itself, an organization might need to deal with the lost productivity and the potential danger of data breaches. Unfortunately, devices are often lost. A study from Kensington found that a laptop is stolen every 53 second. And of the 70 million smartphones lost each year, only 7 percent are recovered. That is why agencies need clear policies about—and solutions for—remotely locking devices and wiping them clean of agency data.

On the hardware front

Implementing the right policies and software are critical for mobile security, but starting with solidly secure devices is also part of the equation. There is increasingly good news on that front. Even employees using their own smartphones, tablets and laptops are likely to benefit from today's advances in mobile security. Here is a look at some of the most important security advances in today's mobile hardware:

Tablets: Tablets suitable for government use today should, at minimum, have built-in features for government-grade encryption, password protection and secure VPN connections, and full device and SD card encryption. It's often wise to invest in optional fingerprint scanners, available for some tablets. Depending on the manufacturer and model, there are many other security features, such as Microsoft's Trusted Boot, Secure Boot and Measure Boot for preventing malware; the Trusted Platform Module (TPM), available on Dell tablets, for ensuring integrity; and BitLocker for better hard drive encryption.

Smartphones: All of the major smartphone vendors have upped their security game. Many phones today provide advanced MDM features that prevent employees from making changes to their accounts on their phone, disable hotspot settings, activate or deactivate tracking and remote locking. Some phones also provide touch-based biometric authentication, enterprise single sign-on, the ability to activate VPN access per application, and the ability to configure Wi-Fi credentials for specific authentication methods used in the enterprise.

Laptops: Security features on laptops are fairly mature, yet continue to improve. At the very least, laptops used by government employees should BitLocker encryption, and for more sensitive situations, the highest level of FIPS 140-2 protection. Other valuable add-ons include smart card and fingerprint readers, a way to physically lock the laptop to a stationary object, RSA SecurID and FIPS 140-2-certified TPM for secure credential storage. For the highest level of security, consider something like Dell ControlVault, which isolates user passwords and credentials on a separately controlled hardware chip.

Table stakes: Policies for mobile security

Walling the best security software and networking tools available are critical to maintaining mobile security, something is bound to go wrong if users don't know what the rules are. The key is developing an easy-to-understand mobile security policy with strict rules about what is and is not acceptable. At the very least, this policy should:

- Require users to enable and use passcodes on all devices, and detail specifics, such as minimum length, complexity and update frequency.
- Require the use of encryption to access official e-mail or data on mobile devices. Explain acceptable encryption methods for both data at rest and data in transit.
- Specify the use of agency-approved mobile device management and mobile application management systems to manage all mobile devices.
- Make clear that devices can't be jailbroken or rooted.
- Explain how your organization plans to keep personal data separate from agency data on the device, and what will happen in case the device is lost or stolen (for example, the device will be automatically wiped clean of agency data but will leave personal data untouched).
- Describe the situations in which an agency can access content stored on the device.
- Describe how your agency will monitor mobile device usage and settings.

Critical technologies for mobile security

The best way to ensure that your agency's data and applications and the devices your workforce uses are secure is by using technology designed for that purpose. The acronyms can get confusing, but each technology serves a slightly different purpose and should be evaluated it its own right. Here's a brief rundown:

Mobile device management (MDM): For many agencies, this is the first line of defense. MDM aims to secure the entire smartphone or tablet from top by bottom. While features in different MDM solutions vary, most can track and inventory mobile devices; provision mobile devices from registration and activation to configuration and patches/updates; distribute software and applications according to permissions set by the organization; authenticate users and enforce password policy; remotely wipe devices in case they are lost or stolen; and protect and track sensitive corporate data.

Mobile application management (MAM): Here's where it gets confusing. MAM shares some of the features of MDM, but generally provides controls more specific to applications. Most MAM products can securely manage an organization's enterprise app store, allowing only authorized users to download specific apps; "wrap" applications in security layers and policies that prevent copy/paste or printing; store fully encrypted data without fully encrypting the device; provide security for both data in motion and data in action; disable applications when needed; remotely update application versions and policies; and remotely control management policies.

Mobile information management (MIM): This cloud-based service syncs files and documents across devices, making it ideal for mobile employees. MIM solutions focus on provisioning and controlling access to data on both employee- and corporate-owned devices and remove problems associated with disparate platforms. Designed to work with MDM and/or MAM, there are many secure, corporate-grade MIM solutions that put security fears to rest.

Dell's focus: Keeping enterprise mobility strategies secure

As federal government continues to embrace enterprise mobility, agencies are faced with continuing security challenges. This includes not only the mobile device—whether it is provided by the government or the employee—but applications and network infrastructure. It's a complex set of issues that can get even more complicated if they aren't addressed in an integrated way.

That's the approach Dell has always used, and continues to use with its enterprise mobility solutions. Using a building block approach, Dell provides agencies with the tools they need to manage and track mobile devices, optimize its infrastructure to securely accommodate mobility, optimize applications for mobile devices, and allow users to securely access the applications, programs and data they need from wherever they are working to remain productive.

Security is the cornerstone of enterprise mobility, and is ingrained in every solution Dell offers. Dell's approach gives agencies full control, from configuration and policy setting to secure access, all from a single management console.

The endpoint—the mobile device itself—is the first line of defense for security. Dell Venue 11 Pro secure tablet is a good example of a highly secure mobile device. It, as well as the Dell Latitude notebook, incorporates a FIPS-compliant physical hardware-based Trusted Platform Module (TPM), which holds the security and encryption keys needed to encrypt an endpoint.

To increase the security of the tablet even further, the Venue 11 Pro also can include a smart card reader, which allows users to prove their identity with an agency-issued personal identity verification (PIV) card.

For notebook users, the Dell Latitude can include a hardware encrypto-accelerator—an extra chip for the motherboard that not only speeds up device encryption, but allows agencies to achieve FIPS Level 3 security. The encrypto-accelerator is part of the Dell Data Protection|Encryption suite.

Another critical part of Dell's modular mobility solution is secure network access. Through its acquisition of SonicWall, Dell's mobile solution now includes Mobile Connect, which provides policy-enforced access to resources over encrypted SSL VPN connections; and Clean VPN, which scans traffic to prevent malware on all authorized SSL VPN traffic before it reaches the network.

Fully protecting agency applications accessed by mobile devices requires Dell's comprehensive Secure Mobile Access solution, which manages and secures access to an agency's applications and data. With this solution, agency administrators can authorize and enforce which mobile apps each user or set of users or devices can access.

Dell's secure mobility solutions work hand in hand with continued innovations from Intel®, which power Dell's devices. At the chip level, Intel's Identity Protection Technology provides strong multifactor authentication. Through its acquisition of McAfee, Intel also now provides McAfee VirusScan Mobile, which blocks mobile devices with malware from accessing the network; and McAfee Enterprise Mobility Management, which provides a host of mobile security features. Intel is working to incorporate these capabilities at the chip level, according to Malcolm Harkins, Intel's Chief Security and Privacy Officer.

Full steam ahead

To provide the most comprehensive and secure integrated solutions possible, Dell recently introduced Dell Enterprise Mobility Management (EMM), which incorporates the most critical aspects of endpoint, network and application security in a secure managed container. While it is focused on smartphones, tablets and other mobile devices, EMM's ability to extend across an agency's desktops and other endpoints is what makes it truly unique. It allows users to access secure government applications the same way regardless of the device used without sacrificing security.

Dell's EMM provides several layers of security:

- It does not allow data to be copied, cut or pasted to applications outside of the container.
- Built-in secure remote access works with an agency's existing VPN to securely connect the container to the agency's network.
- It works with an agency's existing firewall to improve protection across the board.

By keeping up with innovations and using a comprehensive approach, government agencies will remain ahead of the curve.

For more information, go to **http://www.dell.com/learn/us/en/555/mobility-components**

DELL