i360Gov BUSINESS TECHNOLOGY NEWS ANALYSIS i360Gov.com | SPECIAL REPORT | JANUARY 2014

Avoiding The Top Ten Government Mobility Risks

Helping Agencies Embrace Remote Site VDI

Mobile devices top the 'most disruptive' technology list because nearly every employee now uses smart phones or other devices daily, even at work. As defense and civilian agencies strive to deal with the influx of personnel sporting mobile devices, requirements to properly secure mobility continue to grow.

And it's not just employees with 'rogue' devices putting agencies at risk. Government remote site locations pose unique challenges for defense and civilian agencies primarily because data security, administration, even backup and recovery operations can vary greatly at offsite, far-flung locations, and these variations may pose significant risks for data losses or other breaches.

For public and private sector organizations, enabling mobile and remote access to systems and information, no matter where employees are working, remains a thorny challenge. And the unique regulatory requirements faced by government to protect personal information and secure sensitive data, only compound the complexities of enabling access to agency resources. To shed light on the issues, here's a list of the top ten risks agencies face in embracing enterprise-wide mobility. Government organizations must learn to overcome these risks to securely embrace mobility, across the nation and around the globe.

RISK #1: Ignoring the BYOD Influx

Despite a tidal wave of mobile device sales in recent years, the topic of bring-your-own-device (BYOD) security is, at times, still overlooked or ignored in public sector organizations. BYOD is a key disruptive trend that generates serious complications for IT administrators. BYOD policies and procedures must be put in place to properly manage, and control access to government information resources, while simultaneously keeping employees, contractors and others who regularly use mobile devices, productively working. A well-crafted BYOD policy, along with robust centralized mobile device management, can give employees freedom to use their smartphones and other devices to access government networks and information. Some organizations offer tiered levels of access, allowing organization-issued mobile devices to access many resources, BYOD mobile devices running MDM software to access limited resources, and all other BYOD mobile devices to access only a few web-based resources, such as email. Tiered access reduces risks by permitting only minimal access to the least-controlled devices.

RISK #2: Putting Data in Dangerous Places

Growing video traffic, cloud services and the 'consumerization' of IT have forced government organizations to juggle data center consolidation requirements alongside the imperative to improve, not degrade, end-user performance at remote sites and branch offices. As a result, many agencies have been slow to adopt remote site solutions to aid in centralizing/virtualizing access to government resources. However, the risk of security breaches and/or data losses at remote sites and branch offsite locations only continues to grow. It's no longer viable to ignore those risks. New solutions are available to reduce application performance issues, while simultaneously helping agencies gain centralized control of data assets to help them achieve compliance with federal privacy and security requirements.

RISK #3: Falling Short on Mobility Protections

FISMA and HIPPA requirements force agencies to seek stronger security protections, including mobile device management (MDM) solutions. MDM software and services include tools to encrypt data, 'sandbox' or isolate mobile devices, and even wipe clean any devices that are lost or stolen. Additional advances allow for the removal of all data from mobile devices, to avoid even the smallest possibility for data loss or exposure. Specialized encryption, and digital identity management can also render a device useless unless it's properly connected to agency network resources.

RISK #4: Placing Inadequate Emphasis on Virtualization

As government IT executives wrestle with challenges related to serving more employees using a wider array of devices, the need for servers, storage, networking and end-user computing resources that run on a virtualized platform only grows. Virtualization allows managers

continued from "Avoiding the Top Ten Government Mobility Risks..." on page 1

to centralize access to applications, data and desktop delivery processes. In turn, this creates a more flexible, agile environment to efficiently and securely add and maintain mobile devices. Without virtualization, it's far more difficult to embrace mobility, while maintaining security compliance and centralized control over government information resources.

RISK #5: Underestimating Requirements to Improve the User Experience

Early exposure to remote site virtual desktop integration (VDI) left many users unhappy with latency issues, poor/slow performance and reduced usability in some situations. WAN connectivity is key to improving user acceptance. If there are WAN outages, or not enough bandwidth and high latency, meaning lengthy travel times for data from the data center to the user's endpoint device, these elements will hamper the adoption of VDI. Luckily, there are solutions available to address WAN performance and give priority to real-time traffic to avoid degradation. With the right combination of tools and services, agencies can deliver optimized branch office VDI performance, while also enabling centralized management and control of information resources.

RISK #6: Maintaining Mobile Access, With No Centralized Control

The explosion of mobile devices and apps makes it nearly impossible to track what employees will use to access data and information resources without properly configured and centralized mobile device management. Because government employees often must access sensitive, classified or personal information, the National Institute of Standards and Technology (NIST) recommends encrypting mobile device storage so sensitive data can't be recovered by unauthorized parties, or not storing sensitive data on mobile devices. Robust authentication should also be used before allowing mobile device access to internal networks.

RISK #7: Banning Mobile Device Use

This is difficult to enforce, and even considered a 'head-in-sand' approach to mobility that seems ineffectual when nearly every employee owns a mobile device, and the desire to get things done, is strong. BYOD must become a primary focus, to ensure at the very minimum that agencies maintain a 'remote wipe' capability to clear all government data when a device is lost or stolen. Denying or ignoring BYOD use opens an agency to data breaches or losses. With the right policies and MDM in place, it is possible to secure users and devices to ensure government data and resources are protected.

RISK #8: Inadequate Security Awareness Training

Agency employees must be continually educated on risks inherent in mobile device use. Creating awareness programs to educate employees about protecting the organization's sensitive information helps everyone reduce mobile device risks. NIST recommends employees be discouraged from accessing untrusted content with any mobile devices used for work. It is also possible to restrict the use of cameras, or Quick Response (QR) codes. Malicious QR codes could direct mobile devices to malicious websites, for example. Agencies may also choose to disable location services or train users to opt out of location services whenever possible.

RISK #9: Underestimating Protections in MDM Solutions

To streamline desktop and application management, accelerate the provisioning of users and mobile devices, while simultaneously centralizing the management of information resources, mobile device management solutions offer secure mobility for government employees. Virtual devices and applications are run in the data center where it's easier and less costly to test, provision, manage and support, eliminating the need for onsite IT services. Upgrades are seamless, and new applications can be rolled out immediately at the server level. To strengthen security, networks used to authenticate users can be isolated to ensure users only access information resources and applications they are authorized to use.

RISK #10: Skipping Planning and Implementation Steps

Improper design or implementation plans can hinder an agency mobility initiative. Without proper care in design, or in the implementation process, users will avoid, or fail to properly embrace any mandated mobility initiative. Users are key to the success of enterprise mobility, which is why it's so important NOT to skip steps during implementation. The political implications of rolling out mobile access are critically important to maintaining credibility and keeping implementation processes on track.