AVOID MOBILE DATA PERIL:

Route1's MobiKEY technology keeps your data where it belongs — within your enterprise network.

While you're indulging in the convenience of the mobile landscape, you're one step from the abyss of a data breach.

The vulnerability of data is increasing exponentially. Encryption of mobile data at rest, a commonly used attempt at security, is an inadequate measure. After all, encrypted data must be decrypted at some point to be used — and it is at that point that it becomes most vulnerable. Cyber criminals continuously strive to find new ways to hide their malicious code inside mobile apps and websites to lure potential users, sometimes repackaging malicious code within legitimate apps or simply creating new apps that pretend to contain some useful functionality while carefully masking their malicious purpose.[1] A compromised device will expose the decrypted data to the attacker.

Does your mobility strategy compromise the security of your enterprise network? Is your VPN-based approach truly protecting data with which you've been entrusted? How many inbound ports have been opened in your network from mobile users over the past week? Past month? Past year? Do you think, "It won't happen to us" because you stay up to date with your antivirus software? Do you think no one will bother you because you are a small agency? So large that no one will dare? Regardless of your reasoning, you are more than likely at the brink of a security breach that will create a significant loss of data for your organization. This can quickly lead to loss of public and stakeholder trust and can even cost you your job.

A more mobile government workforce is the new reality as mobile technology becomes a powerful tool for productivity. A 2013 Governing Institute survey of government decision-makers found that 90 percent believe mobility improves workforce productivity and increases workforce satisfaction. Eighty-five percent agree mobile solutions reduce operational expenses.[2] But is the risk too great?

Despite its advantages, mobility presents a significant cyber security risk to government agencies. A federal government survey found that 1 out of 3 employees who use their personal devices for work do not password protect their device, and 85 percent download apps which pose a security risk to their data and device.[3] A 2013 report found that as much as 71 percent of cyber incidents targeted users' mobile devices.[4]

Does your mobility strategy compromise the security of your enterprise network? Is your VPN-based approach truly protecting data with which you've been entrusted? You are more than likely at the brink of a security breach that will create a significant loss of data for your organization.

The risk of data being compromised or stolen is high. There are numerous tools and techniques focused on gaining control of an organization's network through downloaded malware, directly stealing information or grabbing data that leaks through nodes created by users, such as when connecting through a VPN. IT personnel are challenged with the impossible task of keeping all the virtual doors locked, while still enabling access to agency data from remote locations.

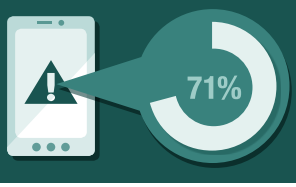
State and local governments need a way to manage mobility and limit risk to take advantage of mobile technology and continue to improve productivity. This Government Technology thought leadership profile dives deeper into the cyber security threats mobile devices pose, why traditional approaches may not be enough and how Route1's MobiKEY technology helps organizations mitigate the risk.

The Risk of Mobility

1 out of 3 federal employees who use their personal devices for work do not password protect their device.

85% of those employees download apps which pose a security risk to their data and device.

A 2013 report found that as much as **71%** of cyber incidents targeted users' mobile devices.



Understanding the Risks: Why Traditional Approaches Won't Suffice

The need for a more advanced mobile security solution is critical in a government environment where employees often require access to sensitive and personally identifiable information (PII). Traditional mobile device management (MDM) solutions are no longer sufficient, especially in a bring your own device (BYOD) environment. It's natural for employees to resist having applications installed on their personal devices that monitor more than their work-related activity. It's unfeasible for contractors and external vendors to accept device profiles, since they can be working for multiple clients and can't share client information.[5] Furthermore, while MDM can provide some level of device protection, when employees leave an agency and take their personal devices with them, any information remaining on those devices becomes unprotected.

By changing the focus from securing devices to securing data, agencies can eliminate the need to manage devices. Solutions exist that cleanly separate personal and work-related activities, and greater visibility, security and control at the document level is now possible, all without managing the device.[6] However, these mobile app management (MAM) solutions require significant IT resources. Someone needs to manage the applications that keep business and personal information separate. Human mistakes can increase the risk of a data breach on the network.

Antivirus software — dedicated to preventing hackers from accessing secure computers — isn't as effective as it should be, even if installed and updated by users correctly, notes Symantec's Senior Vice President for Information Security Brian Dye. Antivirus "is dead," he says, while also estimating antivirus software catches only 45 percent of cyber attacks.[7]

Forty-five percent might even be generous. Antivirus solutions aren't effective because they are reactive instead of proactive in protecting endpoints. It isn't until viruses or malware are introduced to a network that alarms are set off, at which point engineers have to find the issue, contain it and remedy it. Given the pace of malicious data attack adaptation, antivirus developers cannot keep current with the malevolent technical innovation and the sheer number of malicious programs out there.

Here are some numbers to consider: Symantec blocked more than 5.5 billion malicious attacks in 2011 alone, an increase of 81 percent over the previous year. In addition, the number of unique malware variants increased to 403 million and the number of Web attacks blocked per day increased by 36 percent.[8]

Virtual private networks (VPNs), solutions that attach a remote endpoint to the enterprise network — creating a virtual open door — inherently do not offer adequate protection. In order to protect the enterprise network, the endpoint must be malware-free before being permitted to connect. However, it's next to impossible to ascertain that the endpoint is malware-free. Government agencies need ways to restrict or eliminate VPNs because of the immense risk of malware infecting their enterprise networks. Equally concerning are penetration attacks against government networks, whether perpetrated by the criminal element or state-sponsored. The risk of maintaining open inbound ports on the firewall needs to be critically evaluated.

Moving Forward with MobiKEY: Granting Access While Keeping Data Secure

Government organizations and enterprises need a solution that helps them solve the balancing act of ensuring employees have remote access to information needed to perform their jobs while at the same time keeping that information secure.

Many federal agencies, including the U.S. Department of Defense, Department of Homeland Security and Department of the Interior, as well as numerous state and local governments, have deployed the panacea for these requirements: Route1's MobiKEY.

"The MobiKEY solution is better than consumer-driven mobile security access tools because it is a true enterprise-based, yet simple-to-operate tool for users to get back into their work computers. And it's at a higher security level than just about anything else out there."

— Jay Wessland, Vice President and CTO, Boston Celtics

MobiKEY is equally effective beyond the government sector, and is the ultimate solution for mobile data security in the corporate world as well. As the vice president and CTO for the Boston Celtics, Jay Wessland knows a thing or two about the importance of keeping data confidential. He faced a similar challenge as most government agencies when the Celtics' managerial staff started requesting more mobile access to the team's systems. "Getting remote access to legacy apps that were brought into the enterprise was difficult — and difficult to do securely," Wessland says.[9] His organization turned to Route1's MobiKEY, a complete desktop, secure remote access technology that integrates multifactor authentication and identity management in a mobile computing environment, to solve this challenge.

Wessland notes, "Most users, when out of the building, can live on email and they have access to that most commonly on their phone, tablet or easily through Web access from any computer. That takes care of 80 percent of my users' needs when they are out of the office." The access to specialized apps without opening the proverbial door to cyber risk led Wessland to MobiKEY. "MobiKEY ensures a secure remote desktop connection by running in a box on the client and thereby avoiding attacks from the operating system," says Wessland. The organization has now been using MobiKEY to successfully mitigate cyber threats for several years.

Route1's MobiKEY uniquely combines secure mobile access with high-assurance identity validation and plug and play usability. MobiKEY enables the productivity gains of mobile access and BYOD without exposing organizations to the risks of data spillage or malware propagation. Additional benefits of MobiKEY include:

Ease of use. The plug and play functionality offers instant and secure remote access on any device. There is no learning curve for the secure remote access solution itself, and users can immediately access their full office desktop exactly the same as if they were sitting at the office computer. Anything they'd see on the desktop in the office is securely displayed on the remote device. Keystrokes and mouse movements, or gestures, are encrypted and sent back to the desktop.

Unique architectural approach. MobiKEY operates completely clientless and driverless, ensuring no virtual footprint is left behind on the remote device; absolutely no data from the agency's network is ever brought over to the remote device. Best of all, there is nothing to install on the remote asset. No data or files are moved from the organization's network, eliminating the risk of data loss and data leakage. For example, if a user accesses health records or Social Security numbers through a laptop enabled with MobiKEY, and that laptop is later lost or stolen, there is no risk of the data falling into the wrong hands. Once the user terminates the remote data session, there is no footprint to follow. The remote asset never becomes a node on the enterprise network, which means there are no virtual doors that are opened to malware or viruses. The enterprise network and all data remain immune to zero-day threats.

Risk mitigation. MobiKEY offers increased reliability and eliminates the risk of sensitive data accessibility because organizational data never needs to reside on a mobile device. The data never, in any instance, leaves the organization's network. Users accessing data from an agency's network remotely have a full workspace experience from any mobile device — they have full visibility and functionality to work on data and files without introducing any risks to the agency's network.

Enhanced security. The patented technology of MobiKEY offers superior data protection. Its multifactor authentication method inherently limits any ability to imitate the user and gain unauthorized access. Paradigms are enforced that enable user authentication through smart cards or similar principles, depending on the user and the type of device. "The MobiKEY environment runs in its own box and protects our company's data from whatever might be going on at the remote user's location," Wessland says.

Lower TCO. MobiKEY helps agencies lower total cost of ownership (TCO) in several ways. Its technology is delivered as an affordable service, so there is no equipment to purchase or manage; it eliminates capital expenditures and lowers operating expenses. Its subscription-plan pricing is much like a cell phone model, where subscribers can be added and removed easily. By leveraging user-owned equipment, MobiKEY enables agencies to reduce management, maintenance and support costs.

Wessland appreciates the low administrative overhead costs with MobiKEY. "Once I show a user how to set it up one time, which is at most a 10-minute process, I never touch it again," he says, which is unlike any other solution he's found. Wessland notes that other implementations take a lot of care and feeding, need to be touched all the time and are much more difficult to administer.

MobiKEY helps agencies leverage their existing capital investments and enables users to access their full desktop from anywhere, without risk to data.

Still Not Convinced? Consider the Following:

In 2012, the state of Alaska's Medicaid Office was fined $1.7 million after an employee's device that may have contained protected records of Alaska citizens was stolen.[10] A data breach in Utah that exposed over 800,000 residents' health and Medicaid data — including 280,000 Social Security numbers — also caused a renowned CIO his job.[11]

As cyber threats become increasingly targeted, malicious, persistent and designed to acquire valuable information, they have the potential to cause millions of dollars' worth of damage. For example, according to a report from the New York State Attorney General's Office, data breaches that exposed the digital personal records of New Yorkers to potential identity theft and other fraud tripled between 2006 and 2013. "The overall cost of data security breaches is nothing short of staggering," the report noted. In 2013 alone, breaches are estimated to have cost organizations doing business in New York State over $1.37 billion.[12] And in April 2014, the U.S. District Court for the District Court of New Jersey ruled that the Federal Trade Commission could sue companies on charges related to data breaches.[13]

Conclusion

MobiKEY enhances data security so agencies can focus on more strategic initiatives to better improve service delivery to citizens, streamline operations and boost productivity. "The MobiKEY solution is better than consumer-driven mobile security access tools because it is a true enterprise-based, yet simple-to-operate tool for users to get back into their work computers," Wessland says. "And it's at a higher security level than just about anything else out there."

ENDNOTES

1. "Internet Security Threat Report 2014," Symantec, 2013 Trends, Volume 19, April 2014, www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf
2. CDG/Governing Institute Enterprise Mobility Survey, www.govtech.com/library/papers/Top-4-Areas-in-Government-Where-Mobility-Has-the-Greatest-Impact-Whitepaper-.html
3. "The 2013 Digital Dilemma Report," Mobile Work Exchange, 2013, www.cisco.com/web/strategy/docs/gov/digital_dile_rep.pdf
4. "2013 Data Breach Investigation Report," Verizon, 2013, www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf
5. "5 Things You No Longer Need to Do for Mobile Security," Network World, July 7, 2014, www.networkworld.com/article/2451083/byod/5-things-you-no-longer-need-to-do-for-mobile-security.html
6. Ibid.
7. "Symantec Develops New Attack on Cyberhacking," Wall Street Journal, May 4, 2014, http://online.wsj.com/news/articles/SB10001424052702303417104579542140235850578.
8. "Annual Symantec Internet Security Threat Report Reveals 81 Percent Increase in Malicious Attacks," Symantec, April 30, 2012, www.symantec.com/about/news/release/article.jsp?prid=20120429_01
9. All information and quotes from interview with Jay Wessland, July 10, 2014.
10. "Alaska Settles HIPAA Security Case for $1,700,000," HHS.gov, June 26, 2012, www.hhs.gov/news/press/2012pres/06/20120626a.html
11. "Lessons from Utah's Massive Data Breach," Governing, 2012, www.governing.com/columns/tech-talk/col-lessons-cybersecurity-breach.html
12. "Information Exposed: Historical Examination of Data Breaches in New York State," from the office of the New York State Attorney General Eric T. Schneiderman, July 14, 2014, www.ag.ny.gov/pdfs/data_breach_report071414.pdf
13. "FTC Can Sue Companies Over Data Breaches, Court Says," Insurance Business America, May 6, 2014, www.ibamag.com/news/ftc-can-sue-companies-over-data-breaches-court-says-18080.aspx