

The Mobility Paradox

Managing Information Security and Worker
Connectivity in a Global, Mobile World
By Doug Close

The statistics supporting the increased mobility of today's workforce are clear: Eighty-nine of the top 100 U.S. companies offer telecommuting; fifty-eight percent of companies consider themselves a virtual workplace; only nine percent of employees work at headquarters; and sixty-seven percent of all workers use mobile and wireless computing. Add in the Bureau of Labor Statistics estimate that virtually all of the 15 million new jobs in the next five years will be in the services sector, the data will become even more compelling.

While workplace trends might have executives nodding their heads, recent workplace events have them shaking them: A laptop containing Hotels.com customer data was stolen after an Ernst and Young employee left it inside a locked vehicle; the U.S. Department of Veterans Affairs reported that a stolen laptop and external hard drive were to blame in the loss of sensitive information on 26.5 million U.S. veterans; A large mutual fund company lost confidential information on nearly 200,000 Hewlett-Packard Co. employees. A little \$2,000 laptop that is lost or stolen

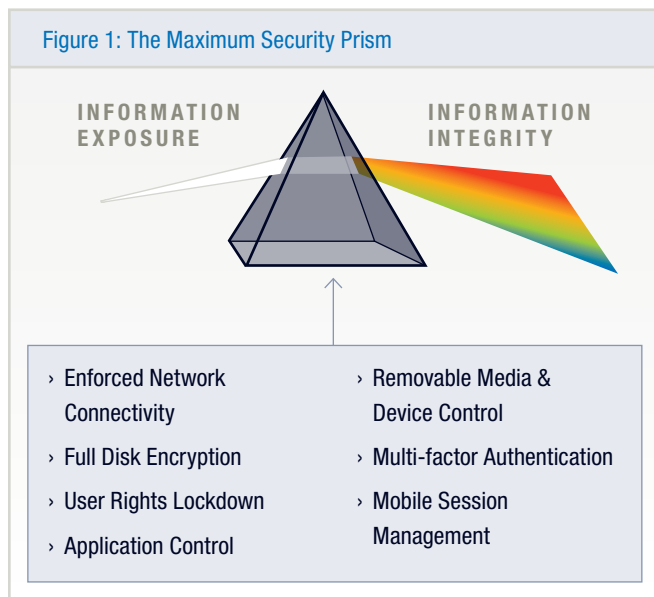
sets in motion a chain of events that has the company IT department scurrying and the corporate executives reaching for antacids. The impact of compromised data is more than expensive. It can devastate a brand.

Today, it is imperative that organizations secure their data and manage their risk... rapidly. At the same time, companies must respond to competitive pressures and use technology to enable higher levels of personal productivity and performance. That means having fast, immediate, 24/7 access to information anywhere in the world. It means delivering connectivity and security, at the same time and without compromise. It means having to manage what I call, *The Mobility Paradox*.

This article will present ideas on how to manage and master *The Mobility Paradox*. We will present security strategies first—beginning with basic and proceeding to advanced—then address connectivity strategies that are congruent with those security objectives.

Security Today

Information security in today's environment is a serious challenge and the mobility of today's workforce makes it, literally and figuratively, a moving target. There is no silver bullet. A carefully managed, integrated approach is required. An intertwined and layered set of strategies can act as an informational prism (Figure 1) and enable substantially higher levels of electronic data integrity. We will review each of the components that make up *The Maximum Security Prism*.



Basic Security Strategies

ENFORCED NETWORK CONNECTIVITY

Mobile devices are exposed directly to the Internet and, without the proper protections in place, can be compromised within minutes. An emerging strategy is to immediately force a secure connection to the company network via a secure tunnel, and firewall other channels of communication to secure the device. This will leverage LAN security systems already in place on the corporate

network and can force all traffic through the network to ensure policies are being met. This strategy is highly recommended for corporate-owned devices that can be brought in and out of the physical company network. Although network access control systems can help identify non-compliant machines, the best approach is to proactively protect devices to keep them in compliance. Technologies today can provide this type of security; they also offer other connectivity benefits including application stability, session persistence, and bandwidth management. While typical IPSec and SSL virtual private network solutions may be inherently secure, they do not provide the overall security solution needed for today's growing base of mobile devices.

FULL DISK ENCRYPTION

For organizations that have corporate data stored on remote devices, full disk encryption is the best method to protect the information and ensure it is not compromised if lost or stolen. Company policy should clearly state the need for encryption of valued and confidential data. In each case, the organization needs to define the value of the information and evaluate the risk of it being compromised. The risk assessment process can be enlightening; many organizations are shocked to understand the value of information and the potential damage if compromised. It is widely accepted within the security community and many regulatory mandates, that full disk encryption is a highly effective approach for meeting an organization's information security objectives. Full disk encryption does not rely on the end user to protect information within remote devices. A properly implemented and documented solution is an effective risk management strategy that will reduce the costs and potential liability in the event of a lost or stolen device.

There are a number of capable full disc encryption technologies to meet the organizational requirements in specific environments. A comprehensive review of those requirements as well as vendor software and service capabilities— such as centralized control, removable media, and integrated directory services—is critical.

USER RIGHTS LOCKDOWN

Though it seems counterintuitive, the end users themselves are often the largest security risks to the organization. Devices that do not limit users from installing applications and modifying device settings (whether intentional or not) can be easily compromised, and proliferate to the company network. Several factors inhibit companies from revoking local rights of users, but most can be solved through system management tools. These solutions provide a centrally managed local agent on the device that can provide proactive OS and application patching, software distribution and removal, asset management, and remote control. Most network management systems are challenged by remote devices not connecting to the organization's physical network, thereby exposing devices that are mobile for long periods of time.

Consider solutions that can provide effective and efficient solutions for mobility management— providing assessment, remediation, patch management, software distribution and removal, priority enforcement, “poison pill” remote disk wiping or encryption, and remote control features required to ensure policy compliance on all laptops. User rights lockdown has benefits beyond security; it reduces support costs and lightens the implementation load for new software projects because the exceptions and variables are greatly reduced.

Advanced Security Strategies

APPLICATION CONTROL

Anti-virus software and patch management strategies are reactive approaches to security that, left alone, cannot stop zero-day threats. Application Control is a proactive strategy that allows an organization to select and approve those applications to run and execute. With application control, other layers of security including anti-virus and patching can be implemented in a non-crisis setting and on a timetable that fits. Application control software can be matched with removable device control technology as part of a software suite. The technology provider must provide an effective approach to identify the information needed to create policy, and demonstrate an ability to control and enforce that policy.

REMOVABLE MEDIA & DEVICE CONTROL

Removable media is a serious threat to organizations today. Devices such as USB memory keys are virtually free to obtain and easy to use. MP3 devices can have hard drives larger than laptops and easily hold the confidential database of an entire company. Not only can these devices easily transfer data, they can be an easy medium to circumvent security mechanisms, whether intentional or not. As these removable devices become more advanced (some can run a whole computing environment within themselves, bypassing all organizational policies), they are emerging as tools for hackers. For example, in a late 2006 promotion, McDonald's in Japan unknowingly gave away 10,000 USB MP3 players contaminated with a Spyware Trojan.

Organizations need to consider controlling all removable media via Infrared, Bluetooth, USB, Fire Wire, Optical CD/

DVD, etc. or they run the risk of leaving an area open to transfer or loss of non-public data. If organizations choose to allow the use of removable media, they must make sure that anything put on it is encrypted, thus making it unusable if lost or stolen. One USB key or MP3 device can walk away with a truckload of sensitive documents or proprietary information. Technologies exist today that can significantly reduce this risk.

MULTI-FACTOR AUTHENTICATION

Standard token technology providing one-time passwords via physical tokens are the mobility standard for most companies today. But higher costs, support, and lack of convenience, are opening the doors to other options. Multi-factor authentication can be measured at several levels, ranging from “what you know twice” to “what you have” to “who you are”, or combinations. The cost generally parallels the degree of security. Emerging technologies—including keystroke biometrics, device identification, texted one-time passwords and fingerprint biometrics—are reducing cost and increasing convenience. These technologies are maturing quickly and delivering contemporary solutions for large enterprises.

MOBILE SESSION MANAGEMENT

Control of the applications and protocols tunneling into networks via mobile devices is yet another exposure to address. Technologies today can provide granular controls over specific communications from the mobile device to the company network (by device or user) and even allocate bandwidth at a granular level. A key step in the process is to eliminate unnecessary computing processes and protocols in order to reduce risk. Also, many mobile users or devices may only need certain functionality based on connection type or bandwidth availability.

Many new applications require LAN type connectivity to function correctly; any mobility solution should take this requirement into consideration.

Connectivity Strategies

MOBILE INTERNET CONNECTIONS

Advanced connection technologies ensure remote and mobile workers are able to stay connected to the people and business systems that are critical to their success. Mobile Internet providers must excel in two critical categories: Unifying Connections and Platform Reliability. Remote users, particularly mobile workers, must have a consistent and standardized way to connect wherever they need to work. Today, virtual network operators are aggregating multiple networks and connectivity types, providing the robust solutions demanded by mobile users. This includes: WiFi, wired broadband, dial, cellular, and emerging technologies like WiMAX through multiple ISPs, company networks, and personal home networks.

For most companies, costs for remote connections are in a “Black Budget” and very expensive, once uncovered. (Some analysts estimate more than 70% of expensed fees are not properly calculated into remote access costs.) Providers must bring these costs into the light of day and provide metrics to demonstrate cost savings. Finally, connectivity solutions must compliment—not compete with—an organization’s mobile security strategies and integrate or interoperate with other security technologies. A remote access solution that provides high availability, real cost savings and information security compatibility will be widely praised by remote users, financial managers and IT professionals—a rare trifecta!

APPLICATION STABILITY AND SESSION PERSISTENCE

While IPSec and SSL VPN technologies offer viable options for securing remote connectivity, they are not designed for today's wireless users connecting to dynamic and unstable public WiFi, cellular data, and campus wireless access points. Technologies today can stabilize corporate applications so that unstable, slow, and frequently disruptive Internet connections do not require multiple re-logins and cause applications to crash. These technologies also provide greatly enhanced throughput for bandwidth intensive applications, as well as Quality of Service customizable policies for not only voice and video, but also priority applications. As wireless connectivity becomes more ubiquitous, the ability to persist and deliver uninterrupted mobile computing across providers will become a mobility necessity.

OVERALL EASE OF USE

Eliminating end user decisions and automating connection technologies will enable mobile users to connect more effectively, and provide greater security by eliminating

potential disregard for policy and standards. Organizations cannot assume that, if certain types of connectivity are not enabled or against policy, their users are complying. Users will always look for ways to be more productive. The best policy to manage this reality is simply to provide the very best mobile connectivity solutions. It is important not to assume "ease of use"; that is something that can only be determined by piloting the solution with real users.

Final Words

The Mobility Paradox is about managing two seemingly conflicting objectives: securing information and making information accessible to those who need it. *The Mobility Paradox* says it does not have to be an "either/or." In fact, it says is not an "either/or", bi-polar measurement at all; it is a new way of looking at managing information in a global, mobile world. Done right, it can become a competitive advantage for any company. Organizations who can master *The Mobility Paradox* will realize that, indeed, it is possible to have your information . . . and secure it too.

Doug Close is Director of Mobility and Security Solutions for Sayers' Advanced Strategies Practice in Chicago