

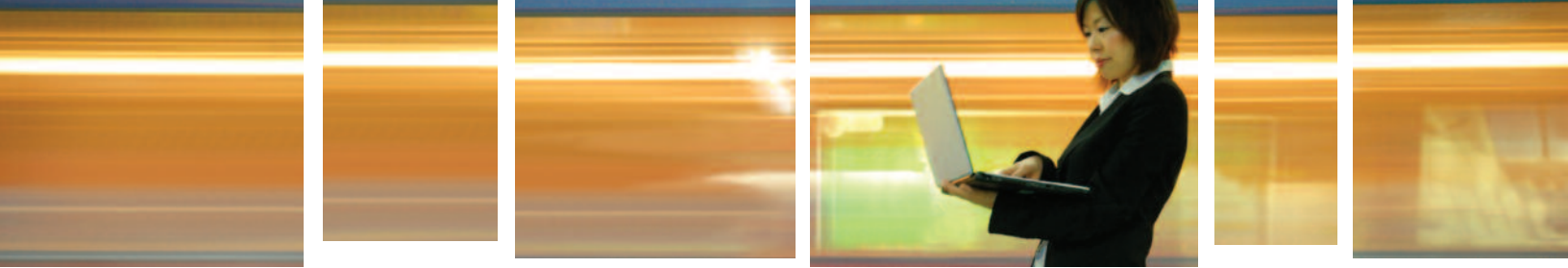


Data Protection on the Move

**Four things every business (small, medium or large) should know about
guarding critical data on mobile computing platforms**

Brought to you by





Data Protection on the Move

Four things every business (small, medium or large) should know about guarding critical data on mobile computing platforms

By Curtis Franklin, Jr.

The Challenge: A Mobile Workforce

The vast world outside the confines of your protective firewall poses a growing threat to the safety of your company's sensitive information. With everyone from CEOs to carpenters taking company networks to customer locations with them, an increasing amount of business takes place in that world.

The data contained on or accessible through mobile devices is much more valuable to the business than the laptop, smart phone or other mobile device that carries it. For that reason, every company must develop a strategy for securing information that takes mobile scenarios into account.

For SMBs, the challenge is even greater: Limited staff and expertise makes them particularly vulnerable to sophisticated adversaries that look beyond the obvious (big banks, for example) to companies they perceive as easier targets. This paper explores the nature of the security problems that accompany highly mobile computing devices and the building blocks for solutions to those problems.

Defining the Threats

The primary mobile information risks come from three types of data breaches: data loss, data leakage and data theft.

Data loss is the accidental release of sensitive information through the loss of the device on which the data resides.

Data leakage is the intentional, though unauthorized, release of sensitive information through the actions of an employee, contractor or other "corporate insider."

Data theft is the taking of sensitive information from an unauthorized person outside the organization.

Taken together, these three categories of data release represent an enormous intellectual and financial risk to the organization. Estimates of the economic impact represented by data release range from \$85 to \$200 per record, and because many incidents involve hundreds or thousands of records, the cost can quickly become astronomical.

Any effective mobile information security solution must involve the four elements described here.

1. Access Control Policies and Technologies

Protecting a company from unauthorized data release requires coordinating responses around four spheres of activity: the people, the policies, and the processes of the business, and the technology used to implement those policies and processes.

Although technology tends to get the lion's share of attention in the press, there's a reason it comes at the end of the list: To be effective, technology must implement workable policies and procedures and must be used by people who understand the importance of information security and the consequences of security failures.

Security begins with access control. Unauthorized data release can't begin to be dealt with until the company has defined who is authorized to have access to data, and what they are authorized to do with the data to which they have access. The most important piece of the access-control puzzle is deciding who should have access to which data. While it can seem a source of unwelcome and unnecessary work, figuring out which job classifications should be able to see and use particular types of data can be worked out in even the smallest company and adjusted as necessary when the company grows.

Company growth and personnel changes are

ABOUT THE AUTHOR

Curtis Franklin, Jr. is a technology journalist with over twenty years' experience covering the computer, networking and communications industries. He has written on a wide variety of topics, with a special focus on security, mobility, and enterprise networking issues.

responsible for the most frequently overlooked aspect of access control: revising control when job classifications or individual assignments change. Many data release incidents are made worse because the individual account or system through which the loss occurs carries the cumulative privileges of every position the individual has held in



Assume that unauthorized individuals will gain access to data at some point. The issue, then, is to make sure the data is not recognizable or useful to anyone who isn't authorized to use it.

the organization, rather than the privileges limited to the position currently held. Making sure that data access and process privileges are revised each time an individual changes positions can solve many security problems before they develop.

Once proper policies are in place, ensuring that the individual using a device is authorized to do so is a matter of technology. Access control tends to be spoken of in terms of “factors,” with two-factor authentication often considered a proper balance between security and user convenience. In most cases, the two factors are something the user possesses — a system, a security token or a fingerprint, for example — and something the user knows, typically a password or PIN. Once both factors are presented, the assumption is that the user’s identity is genuine, and access may be granted.

Options such as HID Global’s naviGo and iCLASS make use of pre-boot authentication capabilities present in laptops from Dell and other manufacturers to authenticate the user, based on a password and either a fingerprint or smart card scan, before the operating system is invoked, guaranteeing that OS password workarounds can’t be used for illicit access.

One of the major issues in access control today is the question of “identity federation” or “single sign-on,” in which users’ identities are established when they log into their laptop computer or smart phone, and then accepted with no further verification by the networks and applications that they use. Individual companies must decide whether the access control mechanisms available on the portable devices are secure and reliable enough to allow them to act as gatekeepers for the enterprise network. Strong authentication mechanisms are available on many devices from a number of vendors such as RSA, with its SecureID token system, and may be sufficient for individual companies to rely on for basic security.

2. Encryption

Although a reasonable level of trust must exist between an organization and its employees, it’s critical to assume that some unauthorized individuals may be able to gain access to data at some point in its life. The issue for security, then, is to make sure that the data is not recognizable or useful to anyone who isn’t authorized to use it.

Keeping data from becoming useful to unauthorized users is the job of encryption. Understanding how and when to use encryption is important for anyone attempting to formulate a comprehensive security strategy for an organization. For those working in industries or locations where regulations such as HIPAA or Massachusetts 201 CMR 17.00 are governing documents, encryption is far more than an option for data protection — it can be seen as a mandatory fail-safe technology in the case of device loss or theft. In any of these cases, it’s especially important to know the differences between the two major types of encryption used in computing: encryption of data in place, and encryption of data in transit.

Encrypting data in place involves the secure encryption of all or part of a mobile device’s storage system. Whole-disk encryption is just that: encrypting every data file on the device as it is stored, and decrypting it as required for use or modification. Whole-disk decryption has the advantage of being secure and simple for the user; there’s no need to remember which part of the disk is encrypted or how to encrypt individual files. The disadvantage of whole-disk encryption is performance, because every file is subject to the additional processing required for encryption and decryption. In terms of security, whole-disk encryption can ensure that no data, no matter how seemingly innocuous, can be used by an unauthorized individual who gains access to the device. With encryption of individual files or directories, the possibility exists that a user will store a file in a wrong directory, forget to encrypt a file or commit another error that leaves the data vulnerable.

There are a number of third-party packages from companies such as Wave Systems, PGP, Sophos, GuardianEdge and Credant that will encrypt files on either a directory or whole-disk basis, and both Windows 7 and Macintosh OS X Snow Leopard offer the capability. Smart phones do not generally come with device encryption as part of the operating system, but products from companies such as PGP, Navastream and GuardianEdge can be applied to some smart phone models to protect the

data in place on the device. With data protected in place, one can then consider the more common case of protecting the data as it moves from one system to another.

Virtual Private Networks (VPNs) are by far the most common mechanism for encrypting data in transit. Whether they are inaugurated through a secure socket layer (SSL) Web-based service or by using a separate program that creates an IPsec (Internet Protocol Security) tunnel using either PPTP (Point to Point Tunneling Protocol) or L2TP (Layer 2 Tunneling Protocol), VPNs securely encrypt all the data that moves between the two systems or networks connected by the tunnels. In general, each VPN connection involves a tunnel pair, with each tunnel allowing data to flow in one direction.

The most vulnerable point in any VPN life is the authentication process at the beginning of the transaction. If the protocols are not handled properly, the initial log-in credential can be sent “in the clear,” subject to theft by a snooping individual. Multiple tunnel types or stacked protocols can help guard against the most basic forms of log-in information theft at the tunnel’s inception.

Encryption can protect against a number of data theft schemes, but data must ultimately be decrypted in order to be displayed or processed.



Protecting systems against malicious virus code was once considered the primary means for guarding a computer's data. Today, anti-virus software is only one of the critical security applications for mobile systems.

Advanced network and end-point attacks can detect and steal data at this vulnerable point. Stopping these attacks is a job that has fallen to protective software, though there is a growing debate about the effectiveness of any software to stop the most sophisticated current attacks.

3. Protective Software

Once upon a time, protecting systems against malicious virus code was considered the primary means for guarding a computer's data. Today, anti-virus software is only one of the security applications generally seen as critical for protecting a mobile system. Software to protect against spam and ad-ware is important, as is a firewall and intrusion detection system. For many organizations, software to protect against Web-introduced threats is important, as are filters for both incoming

and outgoing traffic flagged as malicious. Each of these can be deployed separately, or they can be brought together in a universal threat manager (UTM) that combines multiple protection mechanisms in a single package that attempts to leverage the multiple mechanisms for more comprehensive defense.

Because viruses, worms, trojans and the like tend to be system-specific in their operation, the software to protect against them has been quite system specific, as well. Some operating systems, especially Microsoft Windows, have been heavily targeted by virus writers because of the sheer number of Windows-based computers in the market. As a response, Microsoft now incorporates anti-malware software into Windows 7, and third-party software is available from many companies, including Norton, Symantec, CA, F-secure and AVG. This malicious emphasis on Windows computers has led some proponents of other systems to claim that no anti-malware software is required. While the number of threats to Macintosh and Linux-based computers isn't nearly as high as those to Windows machines, assuming that no protection is needed is a huge leap of faith.

Proof-of-concept viruses and worms have been released for both Macintosh and Linux computers, as well as for BlackBerry, Palm and Qualcomm smart phones. While very few viruses have appeared “in the wild” with smart phones as a target, anti-virus software for various phones is available from a number of companies including F-secure, Norton, Kaspersky and avast! Depending on relative unpopularity to protect a system is a short-term point of view — one that is likely to have negative consequences on extremely short notice.

Anti-malware packages target unauthorized software that tries to become resident on a computer. Firewalls, on the other hand, focus on blocking access to the computer through network ports that might have been inadvertently left open to the outside, or that are required for normal computer use but have been targeted for unauthorized access. Both Microsoft and Apple include firewall functionality in their operating systems, and mobile computer firewalls are available from a many vendors, including Norton, Symantec, ZoneAlarm and Comodo.

Smart phone firewalls are much less common, but are beginning to become available from companies such as Norton, McAfee and Trend Micro. Firewalls are complemented by intrusion detection systems (IDSes) that keep watch on traffic patterns and data-transfer conversations taking place on a system. As the name indicates,

many IDSeS will simply notify a user or administrator that a suspicious pattern of data transfer is taking place, while leaving threat mitigation to the user or another application. Others will move proactively against suspicious conversations, closing network connections or throttling bandwidth to slow or stop suspected malicious activity.

All of this sounds complicated and resource intensive, and it is. Those descriptions explain why so many companies and individuals deploy only some of the protection software listed above, and why a surprising number of organizations feel that protection isn't necessary at all.

The necessity of protective software isn't questioned by most security experts, though its effectiveness at defending against sophisticated attacks is. The question is really one of timing — whether the engineers who develop the code signature and behavioral patterns for the defending software can stay ahead of the criminals who devise ways to get past that same software. In the past, the two have stayed in approximate lock-step, due largely to the efforts of independent security researchers who would discover problems and tell the vendor first, giving them some time to develop and release a patch before sharing details of the vulnerability with the rest of the world. Today, though, a small but important number of researchers say that vendors have not treated their information seriously, so they have begun releasing vulnerability details to the world almost immediately, hoping to force the hands of vendors to patch problems quickly.

As a result, while a suite of protection software is still critical for mobile computers, it is no longer sufficient. Protection software, in the modern environment, is important because it removes the "security noise" from the mix, making sure that the very basic (and quite numerous) probes and attacks are stopped so that security experts can focus policies and surveillance on the more sophisticated modern attacks. Proper encryption, secure authentication, thoughtful processes and effective backups are all just as important as the better-known software for overall mobile security.

4. Backup

In many ways, backup is the forgotten element of mobile data security. It's frequently ignored for laptop and netbook computers, and generally not considered at all for smart phones. This can be a critical error when problems arise that require completely regenerating the operating environment on the device, a step that is often necessary to completely eradicate the more sophisticated

security exploits. In fact, backing up mobile computers has never been easier, with backup applications now built into Windows 7 and Macintosh computers, third-party software available from myriad sources, and a host of low-cost, cloud-based backup services available for large and small businesses, as well as individuals.

Even smart phones are seeing growth in backup options. Backup is built into the iPhone synch routine; products such as Sprite Mobile, PIM Backup and SPB Backup 2 are available for Windows Mobile smart phones, and DataPilot (among others) has backup software that runs on a wide variety of smart phones from various vendors. Lack of software is no longer a reasonable excuse for not backing up any mobile device.

Where to Get Protection

With all the options for protection and the necessity for ensuring that different packages work in concert, integration of security software has grown in importance. System integrators and hardware vendors now play critical roles in

DELL'S ROLE IN MOBILE INFORMATION SECURITY

Dell builds data and system protection into its systems based on a philosophy that rests on four cornerstones: protecting the system and the data while preventing unauthorized access and malicious attacks. Dell's ControlPoint Security Manager allows someone setting up a laptop computer to enable, configure and check the status of software from partners including RSA and HID Global for access control, Wave Systems for full-disk encryption, and Norton or Symantec software for malware protection. In addition, Dell's ProSupport Laptop Tracking and Recovery system will help locate and recover laptop computers that might be lost or stolen. Each of these capabilities can be ordered with all Dell Latitude and Optiplex laptop computers ordered through Dell Business Solutions.

ensuring that the all the software residing on a platform can reliably work together, and that the initial configuration allows for proper implementation of customer security policies.



All security, whether on mobile devices or mainframe computers, must balance ease of use against data protection.

A growing number of customers are turning to system vendors for complete security software installation, choosing the ease of a single point of contact over the (possible) flexibility of self-sourcing their security infrastructure. This is especially true for highly mobile devices, for which remote support and maintenance will likely be the rule, rather than the exception. Dell, for example, combines internal capabilities such as the ControlVault dedicated security chip, on-board fingerprint scanner and pre-boot authentication with preloaded software from partners such as RSA, Wave Systems, Seagate and HID Global to present a unified security front that can be administered through the Dell

ControlPoint Security Manager. A single response point, whether the query is from the user or the support desk, will make the complex topic of mobile security much easier to support in a time-sensitive fashion.

Protection Must Be Used to Work

The rise in mobile device use is largely due to the increased importance of user effectiveness and system convenience. All security, whether on mobile devices or mainframe computers, must balance ease of use against data protection. On mobile devices, the balance will be more critical because of the nature of the devices — a mobile device that's made inconvenient will either be abandoned in favor of another (possibly less-secure) system or see its security system subverted by a user who values convenience more than the IT team does.

Educating mobile users on the importance of security, developing well-considered policies and procedures for secure use of systems and data, and deploying the proper technology to implement the solid policies will help ensure that corporate data doesn't stray far from home, no matter how far the devices on which it lives roam. ★

ABOUT DELL

Dell Inc. listens to customers and delivers innovative technology and services they value. A leading global systems and services company uniquely enabled by its direct business model, Dell is No. 33 on the Fortune 500 list of America's largest companies. For more information, visit www.dell.com or to communicate directly with Dell via a variety of online channels, go to <http://www.dell.com/conversations>. To get Dell news direct, visit <http://www.dell.com/RSS>.