



# 10 Questions to Ask About Your Enterprise Data Security

September 2007

By Bryan Glancey  
with contributions by Matthew Brickey and Brian Wood

Beginning in 2005, the Privacy Rights Clearinghouse started keeping track of reported data-security breaches in the United States. The vast listing of incidents contained in its public database offers a fascinating yet disturbing chronicle of the vulnerability of corporations, private companies, state and federal governments, universities and healthcare facilities. A few excerpts:

- On Christmas Eve 2005, a laptop was stolen from the car of an employee of Ameriprise Financial. It contained customer names and Social Security numbers and, in some cases, Ameriprise account information. About 260,000 customer records were lost.
- An unencrypted hard drive containing names, addresses and Social Security numbers of members of the American Institute of Certified Public Accountants was lost when it was shipped back to the organization by a computer repair company. 330,000 records were lost when the hard drive went missing on May 19, 2006.
- The personal data of current and former students — including classroom roster names, grades and Social Security numbers — was reported stolen on June 16, 2006. The victim was a professor at the University of Kentucky. 6,500 records were contained on the professor's stolen flash drive.
- On July 2006, a contractor working for Advanced Receivables Strategy — a medical billing records company — misplaced CDs containing the names of 260,000 patients, employees, physicians and board members of St. Francis hospitals in Indiana and Illinois. The disks were inadvertently left in a laptop case that was returned to a store. The records were not encrypted, even though St. Francis requires data encryption.
- A backup computer storage device containing the names and Social Security numbers of every state worker in Ohio was stolen out of a state intern's car on June 15, 2007. The storage device also had the names of 225,000 taxpayers. In all, 500,000 records were stolen.

## In the Breach

Between early 2005 and summer 2007, the Privacy Rights Clearinghouse estimates that just over 100 million records had been reported lost or stolen in the United States alone. The organization says that 40 percent of these losses were attributable to laptop thefts and 15 percent to thefts of other devices like PDAs, smartphones, removable media and tapes.

These data breaches cause much more than just embarrassment, of course. Federal regulations like Sarbanes Oxley and the Health Insurance Portability and Accountability Act (HIPAA) can exact civil and even criminal penalties for data breaches. More than half of the states have their own data-security laws and require that customers be notified if their confidential data has been lost, stolen or compromised.

The financial toll of data breaches can be heavy as well. A 2006 study by the Ponemon Institute of actual data-security breaches found that a single lost record costs an organization \$183. Because multiple records are typically involved, the cost of a single data-breach incident averages \$4.8 million. Factors that make up these startling costs include expenses

for customer notification, legal counsel, auditing, public relations, lost employee productivity costs and customer turnover.

Overall, U.S. businesses lose more than \$18 billion a year in data breaches, according to Pepperdine University.

With stakes this high, companies and government organizations are scrambling to strengthen their enterprise data-security applications and policies. As your own company considers ways to bolster data security, it's important to ask 10 key questions about your current data-security defenses and what you need in an enterprise data-security solution.

## 10 Questions

Is your organization prepared to protect your data in an increasingly mobile business world? Consider the following 10 questions:

### 1. Is your security approach device-centric or data-centric?

The explosion of mobile computing and communications devices — laptop sales are now outpacing desktops and the use of PDAs, smartphones and USB devices is accelerating — means that security must follow data beyond the four walls of the corporate offices.

Traditional security solutions tend to be device-centric, focusing on desktops, laptops and the servers that connect them. The rise of businesses mobility has led to the creation of additional point security solutions designed to protect mobile devices like USB devices, removable media and PDAs. But these solutions, too, tend to be device-centric rather than data-centric.

Your security solution should be designed to protect data, no matter what kind of device contains the data. After all, data can quickly travel from secured to unsecured devices. An employee, for instance, might transfer a spreadsheet on a secured laptop to his PDA —and then wirelessly e-mail the spreadsheet to a co-worker's unsecured smart phone.

Securing devices isn't good enough. Instead, an effective enterprise security solution should be device agnostic and encrypt and protect all data throughout the enterprise, regardless of device.

### 2. Can you centrally manage security on all your computing and communications devices from a single console?

Central management of enterprise security is essential. Otherwise, security is left to local administrators and end users, and there can be no enterprise-wide enforcement of security policies. For companies with thousands of employees in hundreds of different locations around the world, no central management means a security perimeter full of holes.

Centrally managed security applications aren't difficult to find. However, if you require several different point solutions for each type of security, there will be several consoles to manage. This can mean higher training costs, more complexity, greater chances for human error, and higher total cost of ownership.

Find an integrated solution that can manage data encryption, firewalls, anti-virus and mobile device security from a single console.

### **3. Does your security application provide 32-bit, whole-disk data encryption and pre-boot authentication?**

Let's take this question in three parts, starting with whole-disk encryption. Your security application should offer the option of encrypting every file on every sector of your hard drives, including deleted files, temp files and other data at rest. As compared to file encryption — which encrypts specific files and requires users to enter encryption keys for access to that file — whole-disk encryption is transparent to the user and requires no other actions by the end user. As the user stores and calls up files, they are encrypted and decrypted on the fly — ensuring consistent, comprehensive security.

Pre-boot authentication is another capability to look for in a security application. Security solutions that let users enter passwords once an operating system like Windows boots up can give hackers access to deleted or temporary files or let them insert a Trojan piece of software. On the other hand, pre-boot authentication requires users to authenticate themselves before they get access to the any of the contents of the computer.

Also look for security applications with 32-bit operating systems. 32-bit systems are able to communicate over the network with a policy server as the user logs in, meaning that security policy is applied in real-time.

### **4. What happens if a mobile device is lost or stolen? Can you do a remote data wipe or lock the device from a remote location?**

The majority of today's security breaches happen when mobile computing and communications devices are either lost or stolen. Proper encryption of a mobile device will help protect the data in the event of a loss or theft, but the ability to wipe the data clean or lock the device from a central location gives added peace of mind that data is unavailable to anyone but the authorized user. Your security application should allow remote administrators to delete data or lock the device as soon as it is reported lost.

### **5. Can you secure removable media and USB devices?**

USB devices — such as iPods, flash drives and thumb drives — along with removable media such as CDs, DVDs and external hard drives have introduced a whole new front in the war for corporate security. Most security applications designed to encrypt and apply security policies to laptops, PCs and other computing devices cannot detect or prevent data from being transferred to these mobile devices — small devices that nevertheless can store significant amounts of data. Before anyone notices, sensitive data can be “slurped” from a computer and the device slipped into a pocket.

Your enterprise security application should allow security policies to be applied to USB devices and removable media. You should have the option to apply policies that do one of three things: Block all data transfers from USB ports; encrypt a file/folder into which data can be stored on the removable device; or encrypt the whole USB device.

## 6. Is your security transparent yet visible? How do you ensure that users don't bypass it?

Transparent security systems don't require users to do anything beyond logging in, so they don't interfere with everyday tasks or impede productivity. These applications are always working in the background, enforcing security policies without forcing users to make decisions about where to save secure files.

Your security solution should not only be transparent, but visible as well. Transparency and visibility are not mutually exclusive. Authentication at the pre-boot phase gives users confidence that their data is protected. Importantly, it also serves as a deterrent to would-be hackers.

Transparent yet visible systems should not allow end users to turn off certain security features. For security to be enforced across the enterprise, security must be managed centrally.

## 7. How do you ensure that your mobile devices stay in touch and in compliance?

Your security application should ensure that mobile devices such as smartphones, PDAs and laptops stay regularly connected to the network so they can download the latest security policies. Policy-control features can be set, for example, to require that smartphones poll the network every few minutes or ask the user to reauthenticate after a few minutes of inactivity.

Your security solution should also provide a security compliance and remediation feature that monitors mobile wireless and wired devices for regulatory data-security compliance and automatically brings the devices back into compliance.

## 8. Does your security application provide the logging and reporting needed to comply with data-security regulations?

To comply with state and federal data security regulations, your security applications must log everything that happens within the security environment. Among the actions you need to log: Proof of when security policies are applied. A log of successful and unsuccessful log-in attempts. Lists of remediation steps that are taken after unsuccessful log-in attempts. The status of the security policies applied to each device. Logging of all administration actions. In other words, your security solution must include a robust logging function.

This information should be readily retrievable in the form of standard and customized reports.

## 9. Does your data security consist of point solutions or an integrated, comprehensive solution that offers encryption for wired and mobile devices, anti-virus, firewall and VPN security?

Security threats can come from many different sources. Most enterprise security solutions on the market today started out as point solutions like firewalls or anti-virus and added expanded protection as customers found new vulnerabilities. The problem is that a collection of point solutions don't allow organizations to create one set of encryption and authentication policies and apply them simultaneously to a wide variety of wired and wireless devices. They are not integrated.

Look for an enterprise solution that's truly integrated — one that allows encryption, anti-virus, firewall and VPN security policies to be applied across a variety of devices from a single console. Integrated solutions offer more comprehensive protection and flexibility in a world of business mobility and newly emerging threats.

#### 10. Is your enterprise security future-proofed?

The data you're trying to protect lies in an enterprise environment that is constantly changing. For starters, there are new forms of data attacks emerging nearly every day. Three years ago, no one thought much about the vulnerability of USB devices, because they weren't very prevalent and couldn't store a lot of data. Today, they represent a common source of data breaches. No matter which computing and communications devices might become popular in the future, your security solution should be flexible enough to encrypt and protect the data inside those devices.

It bears repeating: Your solution should be data-centric, not device-centric.

What's more, your security solution should be scalable to accommodate more users and additional devices as your company grows. As the number of mobile devices multiply, your solution should be able to maintain fast response times and constant availability. Look for a solution with a Service-Oriented Architecture (SOA) for maximum enterprise scalability. SOA is an architectural style where services communicate with each other by passing data from one service to another, or by coordinating an activity between one or more services.

### Unquestionably Secure

After carefully considering these questions, how does the security solution that you're considering stack up? Is your data completely protected, no matter where it resides?

If not, consider an integrated, data-centric solution like Mobile Armor's Enterprise Mobile Data Security™ (EMDS). At the heart of EMDS is a whole-disk data encryption tool integrated into a single-console solution with anti-virus, mobile firewall, VPN and centralized policy control and reporting.

Don't let your organization become the latest entry in the national data-breach database. Take an honest look at your organization's security perimeter, and then take steps to make sure your enterprise data is unquestionably secure.

Find out how Mobile Armor can protect your data at [www.mobilearmor.com](http://www.mobilearmor.com)

**About Mobile Armor** Privately held, Mobile Armor is a St. Louis based leading provider of Enterprise Mobile Data Security. The company develops and markets the next-generation software suite that enables dynamic organizations to fully protect their critical electronic assets. Mobile Armor is owned, operated and developed in the United States. The company's mobile data security solution is certified to meet the standards and guidelines for security set by the National Institute of Standards and Technology (NIST), an agency of the United States Government. Visit [www.mobilearmor.com](http://www.mobilearmor.com) for more information.

