

Plugging the Leaks: Best Practices in Endpoint Security

White Paper
2008

80-11-01601 Revision 1.0

SanDisk®

Introduction

It's hard to open a newspaper or browse the Web without reading about yet another security breach at a major corporation or government agency.

In October 2006, a contract employee at the Los Alamos National Laboratory took classified national security data home with her on a USB flash drive.¹ Over the past five years the IRS has misplaced nearly 500 laptops containing taxpayer information.² From 2005 to 2006, the TJX Corporation exposed the credit card records of an estimated 94 million customers after one of its retail WiFi networks was hacked.³ There are dozens of other stories just like these.

Though these data leaks were different, the cause of each was the same: An insufficiently rigorous approach to endpoint security. Nobody wants to become a headline. By following the practices outlined in this white paper, you can help your organization avoid becoming the next data leak disaster story.

The Data Leakage Epidemic

CIOs generally have a good grasp on how many seats their organization manages, how many nodes are on the network, and how many laptops or smart phones their mobile employees carry. They've hardened their servers against external attacks using intrusion detection systems, packet inspectors, firewalls, and malware scanners. They may even deploy identity management systems that audit and manage the activity of users on their networks.

But when it comes to portable media players, flash drives, memory cards, optical discs, external hard drives and other portable storage devices, most IT managers don't even know where to begin. It's the endpoints of the network where enterprises are most vulnerable to data leakage – and these days, those endpoints are everywhere.

We are in the midst of a data leakage epidemic:

- Nearly half of all organizations were victims of electronic crime in 2006, according to a survey conducted by the U.S. Secret Service, U.S. CERT, and Microsoft. More than a third of the crimes involved copying confidential data to flash drives or portable media players.⁴
- Half of all enterprises reported the theft of a laptop or other mobile device, according to the Computer Security Institute.⁵
- A December 2007 survey conducted by the Ponemon Institute found that four out of 10 employees reported losing a laptop, mobile phone, PDA, or flash drive containing company data.⁶
- In that same study, more than half of employees report copying sensitive information to flash drives, even though 87 percent of those companies had policies prohibiting the practice.
- According to Datamonitor, the average cost of a data leak exceeds \$1.8 million.⁷

Risks and Consequences

Data leaks most commonly occur when employees take work with them on a laptop or a flash drive, only to lose the device or have it stolen. The most notorious case occurred in May 2006, when a Veterans Administration employee had a laptop stolen from his car that contained personally identifiable information for 26.5 million U.S. military personnel (the laptop was later recovered). Since 2005, nearly 220 million records have been lost or stolen, according to the Privacy Rights Clearinghouse, many of them stored on portable devices.⁸

The small size and low cost of media players and flash drives also make them a perfect tool for corporate spies. Cyber espionage now ranks third on the SANS Institute's list of the top ten cyber menaces for 2008.⁹

- The consequences of accidental and deliberate data leaks can be extreme:
- Theft of intellectual property, trade secrets, or proprietary information;
- Loss of confidential business plans and road maps, resulting in the potential loss of sales or first mover advantage;
- Failure to comply with industry and federally mandated standards for data auditing and safekeeping, such as Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), Sarbanes Oxley (SOX), the PCI Data Security Standard, and Federal Information Processing Standards (FIPS);

- Loss of sensitive customer or employee data, possibly resulting in legal liability;
- Potential criminal charges when data leaks violate state or federal law; and
- Irreparable damage to the organization's public image.

In today's business environment, information needs to be mobile. Banning mobile devices outright can both impede productivity and tacitly encourage employees to engage in "guerrilla" storage tactics using their own portable drives.

But simply establishing corporate policies without any means of enforcing the rules or detecting violations is an exercise in futility. Restricting mobile storage to encrypted devices can help stem data leaks, but only if you can also prevent employees from using non-encrypted storage. A comprehensive top-down approach is needed.

Fortunately, there are practices that can mitigate the risks and enable endpoint security for any organization. These practices involve knowing what devices your organization uses and what data it needs to protect, developing policies that fit each role in the organization, and implementing tools that allow you to audit and enforce the policies without restricting employees' productivity.

1. Inventory your hardware

The first step is to audit all hardware and storage devices used in your organization. Better yet, employ software to automate the process by scanning each desktop and laptop on your network, identifying every device that's ever been connected to it. You'll need this information to set policies regarding the kinds of devices employees will be allowed to use and the types of protections they require (see Step 3).

2. Identify sensitive data

Many organizations don't even know what they have to lose. Simply marking all documents as "confidential" is less than useless. As with hardware, enterprises need to complete a thorough inventory of their data, identifying the files containing the most sensitive information – company financials, human resources records, intellectual property, customer lists, and so on.

Look for software that can automate the process by scanning files on network drives and client machines, checking for specified keywords or easily identified strings such as Social Security numbers. Other software may offer real-time scanning of documents as they are opened, or integrate with content filters used to scan outgoing email for leaks of proprietary information.

3. Establish hardware policies

Your organization needs to decide what types of hardware it will accept and what kinds of data need to be restricted. These policies will likely vary depending on the roles and responsibilities of each individual. There is almost never a one-size-fits-all policy solution.

The first step is to decide what types of devices should be included under your acceptable use policies. A good start would be requiring sensitive mobile data to be stored only on encrypted devices. Endpoint security policies must also determine what kinds of smart phones and portable storage devices are allowed to access the network. For example, you may need to ban all portable MP3 players and digital cameras (except for the CEO's, of course).

4. Establish data usage rules

The next step is to establish rules about what kinds of data files can be portable, and how they are treated. For example, some files may be read only, some may be encrypted, and others may be off limits for all but authorized personnel. C-level executives will have different data mobility needs – and require different policies – than the organization's administrative staff, engineers or outbound sales force.

Such policies must be comprehensive enough to protect your organization, but not so restrictive they impede employee productivity. For that reason, many large organizations choose to monitor and log access to sensitive files rather than block them outright.¹⁰

5. Implement a centralized management system

Policies alone won't make your endpoints secure. You need a means to enforce those policies. According to the 2007 Computer Security Institute Survey, half of all organizations suffered thefts of mobile devices and nearly one in five reported a theft of customer or employee data, yet only 27 percent use endpoint security software.

Network-based data leak prevention systems can detect activity at the port level on every machine connected to the LAN, as well as Bluetooth, infrared, and WiFi connections. They can log all attempts to copy or manipulate sensitive files, alert employees who are attempting to read or modify confidential data, and enforce policies – such as only allowing sensitive data to be copied to encrypted flash drives.

Be sure that whatever system you choose integrates into LDAP-based directory services such as Microsoft Active Directory. This will make it easy to modify policies for groups of users at the same time.

Security-conscious organizations will look for a system that allows them to track offline usage as well – comparing mobile data files against the originals to determine if they have been opened, altered or copied to another device.

6. Start at the top

Implementing a comprehensive endpoint security solution across a large organization can take months if not years. But your data needs protection today. Organizations must perform a thorough risk analysis and establish a security hierarchy. Start with C-level executives, business unit directors, and personnel who travel with sensitive data, and lock them down first before moving on to the rest of the organization.

7. Train your employees

The best defense against data leaks is an educated workforce. According to the Computer Security Institute, 70 percent of organizations spent 2 percent or less of their IT security budget in 2007 on awareness training.⁵ Employees should be schooled not merely on how to avoid data leaks and report those that happen, but also on the compliance framework their organization may operate in, such as HIPAA (health care), GLBA (financial services), or SOX (publicly traded companies).

8. Test your IT environment

Leaky data is like a leaky roof; you may not know you have one until it rains. Likewise, you won't know if your endpoint security system is working until you test it – preferably via a third party firm that can probe for weaknesses your IT staff may not have considered. For example, you can install and implement a virtually bullet-proof data leak prevention system, yet still be vulnerable because someone left the door to the data center unlocked, allowing a thief to walk away with all your backup discs.

The End of Endpoint Insecurity

Mobile data is not going away. Data leaks will only get worse and more costly, both in real dollars as well as damage to an enterprise's intellectual property, market leadership, and reputation.

But endpoint insecurity cannot be solved piecemeal, solely via corporate policies or technologies. Only a top-down effort involving intelligent device management, data monitoring, and centralized policy enforcement will plug the leaks, allowing organizations to operate at the speed of business, swiftly and securely.

Notes

¹ "Close Door Policy," FedTech Magazine, http://www.fedtechmagazine.com/print_friendly.asp?item_id=352 and "A Breach in Nuclear Security," Time Magazine, <http://www.time.com/time/nation/article/0,8599,1612912,00.html>

² "Report: 490 IRS laptops lost or stolen over nearly three years," Computerworld, <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9015700>

³ "Breach of data at TJX is called the biggest ever" Boston.com, http://boston.com/business/globe/articles/2007/03/29/breach_of_data_at_tjx_is_called_the_biggest_ever

⁴ 2007 E-Crime Watch Survey, US CERT, www.cert.org/archive/pdf/ecrimesummary07.pdf

⁵ CSI 2007 Computer Crime and Security Survey, Computer Security Institute, <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf>

⁶ "Survey of US IT Practitioners Reveals Data Security Policies Not Enforced," Ponemon Institute, http://www.ponemon.org/press/RC_PonemonSurvey_FINAL.pdf

⁷ "New Report Chronicles the Cost of Data Leaks," Physorg.com, <http://www.physorg.com/news96708147.html>

⁸ "A Chronology of Data Breaches," Privacy Rights Clearinghouse, <http://www.privacyrights.org/ar/ChronDataBreaches.htm#Total>

⁹ "Top 10 Cyber Menaces for 2008," SANS Institute, <http://www.sans.org/2008menaces/>

¹⁰ "Data-leak security proves to be too hard to use," Infoworld.com, http://www.infoworld.com/article/08/03/06/10NF-data-loss-prevention-problem_1.html

Special Thanks

- Feliciano Rivera, executive vice president & general manager, Secuware Inc.
- Paul Pilotte, senior product manager, Vericept

For more information please visit www.sandisk.com/enterprise or e-mail enterprise@sandisk.com.

SanDisk®

SanDisk Corporate Headquarters
601 McCarthy Boulevard
Milpitas, California 95035-7932
Corporate Phone: (408) 801-1000
Corporate Fax: (408) 801-8657
www.sandisk.com

SanDisk, a global leader in USB flash drives, is driving the convergence of secure portable storage, identity management and virtualization through its Enterprise Division to create a comprehensive solution for mobile professionals in enterprises and government agencies.

Today, SanDisk's Enterprise Division offers solutions for securely storing and managing enterprise data, within and outside the enterprise environment.

With the upcoming introduction of virtualization and identity and access management capabilities, SanDisk expects to allow IT managers to boost employee productivity by mobilizing the corporate computing environment through flexible, secure solutions that also reduce total cost of ownership.

SanDisk brings additional expertise to its customers through member companies in the SanDisk Enterprise Solutions Technology Alliance (SESTA).

All parts of the SanDisk documentation are protected by copyright law and all rights are reserved.

SanDisk and the SanDisk logo are registered trademarks of SanDisk Corporation. Cruzer is a registered trademark of SanDisk Corporation, registered in the U.S. and other countries. Other brand names mentioned herein are for identification purposes only and may be trademark(s) of their respective holder(s).