



Putting a Dent in Data Theft

Multilayer IT security defense systems essential to combat wave of data loss, cybercrime and identity theft.

There's no question that today's massive databases provide immeasurable benefits for organizations. They make it easier to manage accounts, they provide the tools to engage in highly targeted marketing campaigns, and they provide insights into customer value and profitability.

But there's a dark side to maintaining vast electronic records: the vandalism or theft of data can wreak havoc on an organization's reputation; it can torpedo revenues and lead to severe sanctions and fines.

"Protecting data is an extremely serious matter. Information security has become a high risk area," says Matthew Thompson, senior manager at the consulting firm Grant Thornton. These days, a glance at the headlines offers chilling evidence that data theft is a growing problem.

In 2006, The Veteran's Administration realized that it had lost a notebook with 26.5 million records. Earlier this year, retailer T.J. Maxx discovered that 45.7 million credit and debit card numbers had been stolen by hackers. Over the last decade, the FBI has arrested thieves attempting to cart off schematics, data sheets, source code and other intellectual property.

The scope of the problem is nothing short of frightening. According to various industry surveys, approximately one quarter of all organizations have been hit by at least one incident of computer theft over the last 12 months. The 2006 CSI/FBI Computer Crime and Security Survey found that virus attacks, unauthorized access to systems, lost notebooks (or data contained on them) and the direct theft of proprietary information are the leading causes of security breaches. The vast majority of violations lead to direct financial losses. In fact, the U.S. Trade Representative office reports that the theft of trade secrets now exceeds \$250 billion annually.

Today, organizations must deploy systems and technology effectively but also develop strong policies and procedures for managing people as well as data. "An organization must understand its vulnerabilities and have a definitive plan in place," says David Rutchik, managing director at Pace Harmon, a Vienna, Va. IT consulting firm. "It must put the proper protections in place but also examine its relationship with business partners and outsourcing providers."

Building Barriers

Protecting computer systems isn't a new concept. However, the introduction of the Internet and highly integrated networks has ratcheted up the stakes and made the task far more complex. Increasingly sophisticated thieves — many working within highly organized cybermobs — rely on a variety of techniques to steal data, including brute force intrusions, infecting computer systems with malware, stealing notebook computers and planting thieves within organizations or finding an employee willing to cooperate.

With so many points of vulnerability, organizations must develop a security policy that encompasses physical security, authentication tools, intrusion detection, antivirus and malware protection, and training so that employees do not succumb to increasingly common social engineering schemes, such as phishing.

Many employees still fall victim to authentic-looking e-mail messages that lead them to a bogus site, where thieves steal logon information. More targeted spear fishing targets a specific individual and may provide enough real information to make the message seem authentic.

One of the biggest problems organizations face is ensuring that all bases are covered. "In many instances, companies use excellent security tools and have solid processes in place," Thompson explains. "But they overlook a single aspect of security and a hacker or thief is able to slip through a crack." Something as simple as allowing employees to use iPods can lead to data theft; or something as basic as putting up a test system without adequate security controls and protection can allow hackers entrée to company secrets.

Physical security is at the center of protecting an organization and its data. It's vital to have an access control system in place to control entry and exit — including entry gates and warehouse doors. An organization must monitor visitors and third-party consultants that have access to office areas and personal computers. It's also important to block features on systems when they're not needed. For example, a growing number of IT departments block the use of media drives and Universal Serial Bus (USB) ports in contact centers and other locations containing confidential data.

Yet, even with physical security measures in place, an organization must remain vigilant. An ongoing problem is poorly designed or inadequate authentication systems. Many companies continue to rely on basic password protection for file and system access.

Unfortunately, it's not uncommon for people to share passwords or write them down on a sticky note where others can see them — despite ongoing warnings to keep the information confidential. What's more, many organizations allow employees to use weak passwords or retain the same password for years.

As a result, organizations are increasingly turning to token-based authentication. A growing number of companies now market USB token devices, which fit on a keychain and provide instant authentication via the USB port. Because a person is logged on only when the token is present, the device is able to monitor access on a constant basis.

A USB token also allows administrators to store multiple codes on the same device, thereby fortifying protection for restricted applications and files. Finally, many devices now handle both private keys and digital certificates within the same token, creating so-called two-factor authentication.

An individual must use the device and a master password to gain access to the network, the Web, remote Virtual Private Networks (VPNs) and other enterprise applications. Once logged on, there's no need to produce additional passwords for different accounts.

Essentially, the tokens allow a person to work securely from any PC in any place within the enterprise, and network administrators can instantly know who is downloading what data. Numerous companies now manufacture these device. "Tokens create a far more secure network and »

provide enterprise-wide protection," states Shlomi Yanai, vice president of Aladdin Systems.

Against the Flow

Every organization must strike a balance between business needs and security requirements. If controls are too tight, workers can't do their jobs and productivity suffers. If security is too loose, a break-in or breach becomes almost inevitable. Today's data security strategies focus on the use of well-established tools and sound policies rather than cutting-edge solutions.

Centralized logging, filtering, authentication and other network controls are critical — along with a management console for overseeing the status of various security functions. Virtual private networking is imperative for remote workers.

However, the protection can't stop there. Companies are increasingly turning to rights management services (RMS) or digital rights management (DRM) to control sensitive documents and files. These systems, built into Microsoft Windows Server 2003 and available through third-party applications, control who views a file; how long the file is accessible; the ability to alter it; as well as permissions for copying, e-mailing and printing. The software prevents files from falling into the wrong hands or someone losing track of them.

Another layer of protection is encryption. Applications such as Microsoft Outlook offer built-in certificates, password protection and encryption support. It's also possible to use encryption tools from PGP and other vendors to lock down documents and keep them away from prying eyes.

Finally, Microsoft's BitLocker Drive Encryption is built into Windows Vista Enterprise Edition. It stores encryption keys and passwords on a dedicated Trusted Platform Module chip rather than software files that are easy to access and hack. If an employee loses a notebook computer, for example, the hardware is lost but the data is not.

Yet, despite advances in encryption tools, many IT administrators and business executives face ongoing problems. That's because security tools are only as good as the people using them. Too often, individuals forget to encrypt sensitive data — a huge problem when a notebook computer carries proprietary data or customer records.

If the PC is lost or stolen, thieves have instant access to the hard drive and all its contents. "If a computer falls into the wrong hands and the data is accessible, there's almost nothing you can do," says Michael Cobb, managing director of security consulting firm Cobweb Applications Ltd.

As a result, hard drive manufacturers have introduced drives that offer full-disk encryption. In October 2006, Seagate introduced its DriveTrust line. The device automatically encrypts all the data written to the disk, making it inaccessible to anyone who lacks the correct password when the computer first boots.

What's more, because the encryption is built directly into the drive, it encrypts and decrypts automatically and there's no performance lag. Maxtor and other manufacturers have also introduced such drives.

Cracking the Code

Over the last few years, viruses, Trojan horses and other malware have become a plague on enterprise computing. What's more, these bits of code have become far more sophisticated. Zero day exploits now target vulnerabilities as quickly as they become known, and polymorphic viruses change their form and characteristics — thus making them difficult to track down and eradicate.

According to the 2006 CSI/FBI Computer Crime and Security Survey, virus attacks are the single greatest source of financial losses within corporations. In fact, nearly two-thirds of organizations found themselves under attack.

Preventing malware from infecting computers is challenging. Instant messaging and e-mail serve as common carriers for viruses, though it's also possible to infect a computer by visiting a malicious Web site. Phishing schemes routinely trick users into visiting sites that may not only steal identity information but also plant keyloggers, rootkits and other software on computers.

Administrative capabilities and system-wide controls are now essential. Symantec's AntiVirus Corporate Edition, for example, offers cross-platform protection, centralized policy management and lock-down capabilities within a highly scalable framework.

Likewise, an enterprise must ensure that it has a system in place for installing patches to the operating system and various applications — and developing rules and procedures to manage the process across the enterprise. "System vulnerabilities essentially create an open door for hackers and thieves," Pace Harmon's Rutchik says. "Unless patching is applied on a timely and consistent basis an organization is putting itself at great risk."

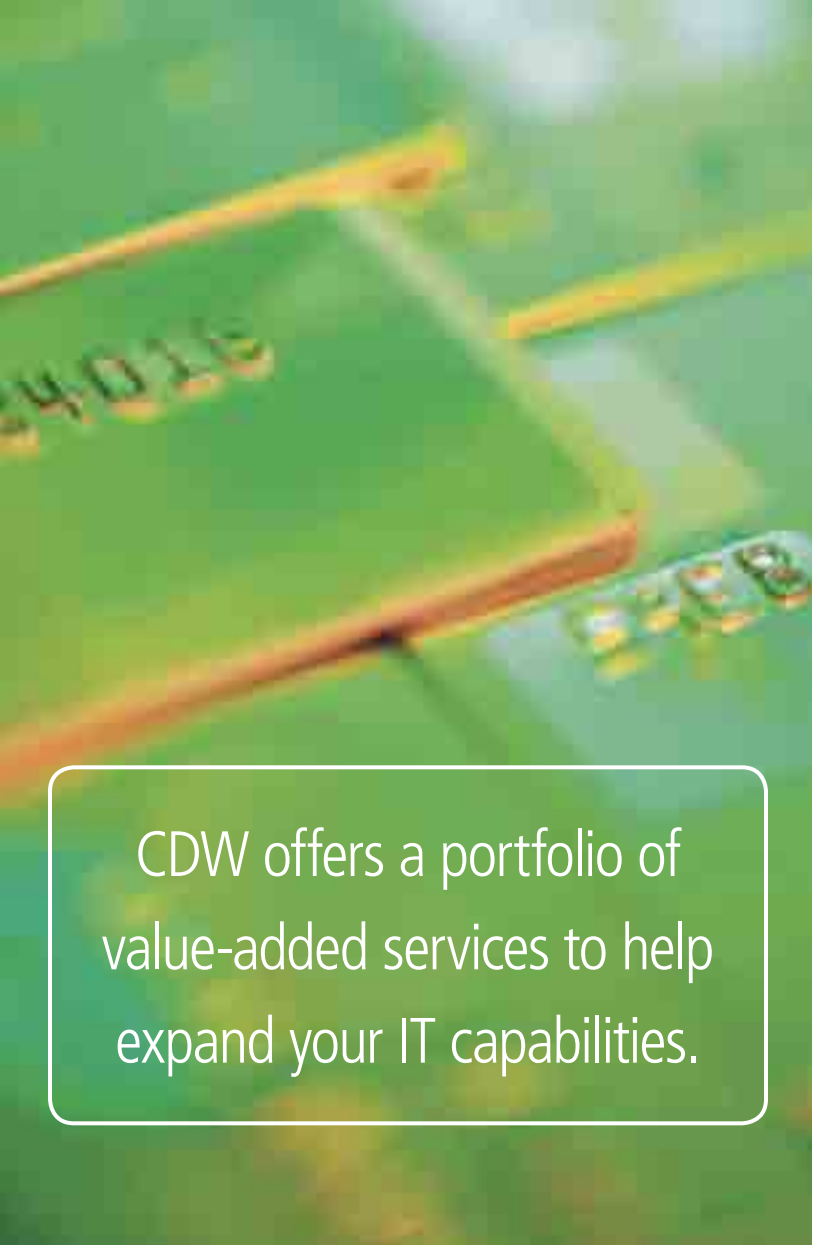
Gaining Control

Developing an effective data protection strategy requires business and IT leaders to understand the value of data, the risks involved with losing it and the potential cost of a breach. "No two industries or businesses are alike. Everybody has a different threshold of pain," observes Grant Thornton's Thompson.

For a law firm, the loss of key e-mail messages could endanger work and undermine a client relationship. For a health maintenance organization, patient privacy may reign supreme; and a lapse could lead to bad press and severe penalties under the Health Insurance Portability and Accountability Act (HIPAA).

Meanwhile, a retailer may find that the loss of customer records — including credit card numbers or Social Security data — leads to customer defections, fines and other penalties.





CDW offers a portfolio of value-added services to help expand your IT capabilities.

“An organization must know where data is kept, how employees store information and how it is exchanged internally and externally,” says Cobweb Applications’ Cobb. For some organizations, including financial institutions, scanning outgoing data for certain numerical strings — including account information or a Social Security number — might top the list. For others, such as a call center operation, blocking incoming e-mail attachments might prevent malware from seeping in and valuable data from streaming out.

Not surprisingly, companies that fail to act or take the threat lightly are likely to find themselves in the crosshairs. Says Thompson: “When a business understands its risk profile and what assets it needs to protect, it can set up appropriate controls. It can greatly reduce the risk of a break-in or theft.” ◇

In the Cards

In recent years, credit cards, debit cards and payroll cards have become a ubiquitous part of society. They’re fast and they’re convenient. However, they also represent a substantial risk. Companies that lack appropriate protections may offer thieves entrée to valuable corporate data, including customer information.

Make no mistake, thieves are increasingly adept at extracting credit and debit card information from unsecured databases, stolen notebooks and other means. The result: an emerging pandemic of identity theft. According to the U.S. Department of Justice, 3.6 million U.S. households — approximately 3 percent — have been hit by identity theft.

As a result, American Express, Discover, MasterCard and Visa have introduced regulations to help thwart the theft of customer data.

The PCI DSS (Payment Card Industry Data Security Standards) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

The standards carry different names for each of the credit card issuers — and all have created their own specific compliance requirements, along with bank and merchant rules and penalties. These range from how data is stored to how and when validation codes are used.

Participating companies can be barred from processing credit card transactions, the card companies can apply higher processing fees; and in the event of a serious security breach, fines of up to \$500,000 can be levied for each instance of non-compliance.

According to PCI Compliance Guide, only 49 percent of banks and merchants are compliant. Approximately 17 percent aren’t compliant and 33 percent are working toward compliance.

PCI DSS Specifics

The Payment Card Industry Data Security Standard version 1.1, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The core of the PCI DSS is a group of principles and accompanying requirements including:

- Build and Maintain a Secure Network
- Protect Cardholder Data
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

For more information, visit www.pcisecuritystandards.org.