

**Data Breaches:
Turn Back the Tide**

Data Breaches: Turn Back the Tide

An information-security best practices primer to minimize the risks posed to business and customer information

Executive Summary

Despite the hundreds of millions of dollars that organizations have invested in information security technology to secure their critical business-technology infrastructures, the bad news keeps breaking. In the past year, dozens of companies have had to inform their customers that the exposure of their personally-identifiable financial information had placed them at great risk of identity theft. The incidents range from fraudsters successfully establishing bogus access accounts to steal legitimate consumer information to hacked networks to lost backup tapes containing the financial information of millions of consumers.

It's not just the widely-publicized cases that count. In the past several years the federal government has prosecuted individuals for criminally abusing their insider access. In February of 2005, federal prosecutors indicted an IT manager for gaining unauthorized access to his former employer's network to read e-mail and causing damage to its systems. Federal prosecutors have also prosecuted and found employees guilty of password trafficking, selling customer financial information—including detailed credit reports—to organized crime.

Recently, IT managers and even customer service representatives, have been prosecuted and convicted for using their privileged access rights to destroy or steal their company's information and selling customer financial data to organized crime. High-tech companies aren't immune, as even network equipment and software manufacturers have had their proprietary source code stolen and made accessible on the Internet.

The sheer scope of the impact is mind-boggling. A recent security breach at a major credit card processor reportedly exposed more than 40 million card-holder names and account numbers. In February, a well-known information-broker revealed that criminals had managed to steal the names, addresses, and Social Security numbers of as many as 145,000 individuals by using previously stolen identities to create 50 fake businesses to access the company's information stores. In another widely-publicized breach, one of the country's largest information services providers announced that hackers managed to gain access to a database to seize the names, social security and driver's license numbers, and addresses of more than 300,000 individuals. According to Gartner, 9.4 million U.S. adults were identity theft victims between May 2003 and April 2004. Their financial losses totaled \$11.7 billion.

Such data breaches have been announced by some of the country's well known banks, entertainment companies, telecommunications providers, and universities. And this proves that such breaches can occur at even the most security conscious and diligent companies. The public is learning about security breaches today largely due to California's Breach Disclosure Law (SB 1386), which went into effect July 2003 and requires companies, with customers who live in California, to make notification if their personally identifiable financial information may have been accessed without authorization. Expect more security breach disclosures when a federal law similar to SB 1386 becomes law.

According to Gartner, 9.4 million U.S. adults were identity theft victims between May 2003 and April 2004. Their financial losses totaled \$11.7 billion.

The human-toll of identity theft on individuals is severe. According to the Identity Theft Resource Center it takes the average victim about 600 hours to prove their identity was stolen and clean their credit reports. And it can be years before most victims attain their financial health. Many victims of identity theft run into trouble getting mortgages, car loans, credit lines, and even employment with a tarnished credit report. In 2003, the Identity Theft Resource Center surveyed 173 identity-theft victims and learned that 4 percent of victims discovered their identities were stolen when they were arrested for crimes committed in their “name.”

Those statistics are even more alarming when one considers that in 2004, the Federal Trade Commission said 635,173 identity theft related complaints were reported. That figure is considerably higher than the 403,688 filed complaints in 2002. It's no surprise consumers are losing trust in E-commerce and how carefully organizations protect their private information. Gartner says 1 in 20 adults are likely to become victims of some form of identity theft.

It's not just consumers that are losing. According to a survey conducted by the Chamber of Commerce, PricewaterhouseCoopers, and ASIS International, businesses lost between \$53 billion and \$59 billion between July 1, 2000 and June 30, 2001 due to the theft of their intellectual property.

Set the regulatory demands on information security aside—Basel II, European Union Data Protection Directives, GLBA, HIPPA, SB 1386, and Sarbanes-Oxley—as customers become increasingly security and privacy savvy, sound security policies and trust will increasingly become a competitive differentiator. Gartner predicts that if Internet-based security threats aren't mitigated, the robust 20 percent annual E-commerce growth rates will be slashed to 10 percent or less within the next two years.

While the myriad of regulations do not dictate what security technologies companies need to set in place, they all demand that business and customer data are adequately guarded.

While it is not possible to eliminate risk, clearly more needs to be done by organizations to reach a higher level of security to protect their intellectual property and their customers' personally identifiable information. The level of diligence organizations place on securing their business-technology systems simply isn't high enough—and is one of the primary reasons identity theft cases are soaring. Organizations need to re-evaluate their approach to information security, consider new tactics for protecting digital assets and, most importantly, the trust of their suppliers, partners, shareholders, and customers.

Organizations Need to Get Back to Basics

To turn the tide on the skyrocketing lack of trust customers have toward the way enterprises protect their personal information, organizations need to instill security awareness throughout their enterprises. Security culture within an organization needs to flow from the top down: CEOs, boards of directors, and senior management need to make it clear that information security needs to be an integral part of their daily operations, and that IT security initiatives must be closely aligned with business objectives. Without senior management providing strong security governance, insiders abusing IT resources, system breaches, and careless handling of customer information will continue to proliferate at an alarming rate. Security policy can't be static; information security policies and procedures need to be dynamic, living documents that

According to a survey conducted by the Chamber of Commerce, PricewaterhouseCoopers, and ASIS International, businesses lost between \$53 billion and \$59 billion between July 1, 2000 and June 30, 2001 due to the theft of their intellectual property.

are continuously refreshed as both technology, computing infrastructures, and business environments evolve.

In a successful information security program, all three pillars—people, process, and technology must be strong. Senior management lip-service to the importance of security, and the protection of the customer information they are entrusted to secure, no longer suffice. The continuous spate of data breaches clearly shows that simply investing in conventional defenses such as anti-virus programs, content filtering, firewalls, identity-management, and intrusion detection and prevention systems aren't enough. Not enough attention is being placed on the other two pillars of security: people (security training and awareness), and process and procedure (security policy), and no amount of investment in security technologies will make up the difference in the equation.

According to Ernst & Young's 2004 Global Information Security Survey, less than half their respondents provide regular IT security training to their employees. Only one-fifth of respondents believe their enterprises view IT security as a CEO-level priority. The 2004 Computer Security Institute/FBI Computer Crime and Security Survey, which queried nearly 500 organizations with arguably the most sophisticated IT security programs, revealed that, on average, all the respondents believed their organizations invested inadequately in security awareness programs. And these organizations invest heavily in many conventional security defenses: anti-virus programs (99 percent), firewalls (98 percent), server-based access control lists (71 percent), and IDS systems (68 percent). One of the most startling statistics from the survey is that even these companies fail to invest in encryption solutions, with only 64 percent encrypting data in transit, and 42 percent using encryption to protect stored files. This raises concerns about just how seriously companies take the task of protecting their own information and the information of their customers'.

Information Security Best Practices

Information security managers are well aware of the best practices outlined below. But the question remains: Why aren't companies better able to secure their intellectual property and the sensitive information they hold about their customers? Because attaining adequate levels of security is extremely challenging and requires a daily enterprise-wide commitment starting at the highest levels of management. While there is no IT security cure-all, information is ubiquitous, and since organizations will continue to increasingly inter-connect their customers, partners, and suppliers to their business-technology systems more must be done. The biggest obstacles to IT security within organizations today are the lack of senior managements' commitment to drive a "culture of security" and set the proper tone throughout their enterprises, a lack of employee security awareness training, and a failure to consistently adhere to strong security best practices and procedures. By doing so, embarrassing and costly data breaches could be greatly reduced.

To help mitigate data breaches, organizations need to:

I. Classify and Determine the Value of Data and Business-Technology Systems

Security professionals know that before any data can be cost-effectively protected, it must first be classified. The first task in risk assessment is to identify, assess, classify and then decide the value of digital assets and systems. Many executives consider the most difficult aspect of a risk assessment is to uncover the abundance

of system and configuration vulnerabilities that place their systems at risk. Not so: An abundance of tools are available to help automate that task. It's deciding, organization-wide, the value of their data and intellectual property that is one of the most daunting tasks security professionals confront. How much is the research and development data worth? How much will it cost the organization if it loses access to the accounting or customer-relationship management systems for a day? Without knowing the value of information, and the systems that ensure its flow, it's impossible to make reasonable decisions as to how much should be invested to protect those systems and information. It makes little sense to spend \$200,000 annually to protect information that wouldn't cost an organization more than \$25,000 if it were exposed or lost. Tough decisions relating to the value of information need to be made. And that means bringing together management, legal, human resources, physical security, and other groups within the organization.

II. Adhere to Network Security Basics

Good network security comes down to allowing only authorized access—both people and devices—to computing systems. The firewall is the cornerstone of network security and serves as the gatekeeper between one network and another (between a trusted corporate network and the Internet or the networks of business partners, customers, and other members of the extended enterprise). Enterprise networks should regularly undergo a risk assessment. As part of the risk assessment, security managers need to identify and then classify, each portion of their network and its risk level, and then dedicate the appropriate levels of protective security controls. High-risk systems include those that if compromised or destroyed, could lead to significant business disruption, or give rise to potentially serious financial and legal repercussions. Because of their function within business-technology infrastructures, the following types of devices and systems are typically high risk: network routers, firewalls, and database and application servers.

Virtually every type of network-connected system should be classified. Once risk levels have been assigned to networked devices, it's time to determine which types of users need access to those systems. Typical user sets include: administrator/privileged users, employees, business partners, as well as customers and other external users who may need limited access to internal systems.

The goal of network risk assessment is to maintain the delicate balance between security and adequate access to business systems. Networks should undergo regular risk analysis. Any changes to a network which could result in lowering an organization's security posture should always be reviewed by security managers. These include changes to firewall configuration and alterations to access-control lists (ACLs). Current software versions should be maintained on all servers and network equipment.

III. Strictly Maintain Strong Application Security Processes

The security watch group, the CERT Coordination Center, estimates that 99 percent of all security intrusions result from the exploitation of system configuration errors and known vulnerabilities within software applications. Gartner reports that organizations that incorporate a vulnerability management process will experience 90 percent fewer attacks than organizations that invest the same resources into intrusion-detection systems.

One of the most effective ways to mitigate risks to business-technology systems is to regularly (weekly, monthly, quarterly depending on asset value, threats, and organizational risk-comfort levels) scan applications for known software vulnerabilities. As soon as a software vendor publishes a software update, or “patch,” enterprises should immediately begin the patch testing and deployment process. Hackers begin developing software exploitation codes within hours or days of a software vendor issuing the patch. Attackers now create worms, and automated software attacks known as “exploits” within a month of public disclosure of a vulnerability.

IV. Maintain Adequate Employee and Physical Security Precautions

While worms, viruses, spyware, and other Internet-based attacks capture headlines, it is employees and other insiders who have access to trusted systems who have the potential, through malice or neglect, to cause great damage. While many business managers fail to correlate physical security with IT security, there’s virtually no IT security if physical access to business systems isn’t controlled. Internal cameras should be placed in hallways leading to the data center or other areas leading to and around data-critical servers. Security policies relating to how visitors enter and exit premises need to be established and enforced. Careful attention should be paid to the physical security of the datacenter. Entrances to the datacenter should be limited. Enterprises which have not implemented strong authentication, such as biometrics, smart cards, or proximity badges to strictly enforce access to the data center, should seriously consider doing so.

To mitigate potential insider abuse, new hires and contractors should undergo a thorough criminal background check. Employment, education, and motor vehicle histories should be carefully researched. Sufficient drug-screening and the verification of social security numbers should be conducted. While it may not be necessary to conduct background checks after an employee is hired, human resources and management should be trained to detect behavioral changes that could result in an update investigation into an employee’s background.

V. Effectively Create and Manage Passwords and User Accounts

Passwords remain the primary key used to unlock access to business-technology systems. Unfortunately, many applications known as password crackers, are widely available on the Internet and can crack most commonly used passwords in seconds. It is critical organizations establish and maintain effective password management policies and procedures from account/password creation, management, and eventual retirement of password-protected accounts.

Given enough time and resources, most passwords can be discovered by a motivated attacker. Aside from the most easily guessed passwords in use today and “dictionary” attacks used to gain access to resources, there are keystroke loggers, worms, and Trojan horses specifically designed to gather passwords and account- access information. The weaker the passwords an organization uses, and the longer the same passwords are in place, the weaker this method of authentication becomes.

Strong passwords consist of more than eight alphanumeric characters. They do not consist of words found within a dictionary of any language or within common slang. Passwords should never be the names (not even spelled backwards) of friends, family, pets, vehicles, movie characters, social security numbers, birthdates, or any other sliver of information remotely associated with the end user. Strong

password construction includes employing both upper- and lower-case characters, and should also include a combination of letters, numbers, and special characters such as #@%^~. Passwords should never be written down on paper and hidden in desk drawers, or under keyboards or mouse pads.

Passwords need to have limited use-life. System-level passwords, such as those used to gain access to networking equipment and server/application administration need to be changed at least every three months. All privileged or “super” user passwords should be centrally maintained and managed in a secure database by the security management team. Basic employee passwords used to access business applications, computers, e-mail accounts etc., should be similarly recycled every 120 days. Despite widespread knowledge of sound password policy, many organizations still fail to adequately create, manage, and retire their usernames and passwords effectively.

VI. Implement Employee Security Awareness Programs

Every employee should be security trained. Employees need to understand relevant aspects of their organization’s IT security policy. Certainly not every employee needs to understand cryptography, security systems architecture, or the nuances of forensic security investigations. But more organizations need CEO-level tone setting when it comes to the important task of protecting proprietary and sensitive customer information. Employees should be well versed in the risks of spyware and downloading unauthorized applications from the Internet and opening attachments; and they should be on guard for social-engineering techniques designed to pilfer usernames and passwords from unsuspecting users.

VII. Secure Data-at-Rest

Given the continuous news of lost backup tapes and unauthorized access to corporate databases, more attention is being given to the effective encryption of “data-at-rest”—that is information stored on desktops, notebooks, PDAs, backup tapes, and storage arrays. The goal of encryption is simple: make data unreadable to anyone who doesn’t have access to read it. Encryption systems use digital keys, which are used to lock information (make the data unreadable) and unlock information (return the data to readability). Without the exact keys, it’s nearly impossible to turn the gibberish into comprehensible text. In the event of a security breach, encryption can be the final layer of defense. That’s why organizations need to design an encryption strategy that is both effective and unobtrusive to normal business operations. Nonetheless, enterprises need to decide how to protect data residing in servers, applications, and other storage devices. Once organizations have completed their risk assessment, classified their information assets, and determined their most sensitive information, they need to ensure their most valuable and private data is encrypted and stored in a highly-secure location. Encrypting stored data can be one of the most critical facets of an organization’s defense-in-depth strategy, but must not be deployed in a vacuum. Encryption needs to work in conjunction with strong network security practices, identity authentication, and policy-based data access controls.

VIII. Secure Data-in-Motion

Securing data while it travels between applications, business partners, suppliers, customers, and other members of an extended enterprise is crucial. As enterprise networks continue to become increasingly accessible, so do the risks that information will be intercepted or altered in transmission. As a result of continued

high-profile information breaches, enterprises will increasingly strengthen the manner in which they encrypt information as it travels throughout their internal network and to the remote networks of their customers and partners. There are many ways to encrypt data in transit, including virtual private networks, and multi-purpose security appliances, which incorporate IDS, IPS, firewalls, anti-virus programs, and other security technologies into a single device. Another option is server-based encryption solutions provided by router and switch manufacturers. Networking equipment manufacturers such as Cisco and Juniper are increasingly enhancing the security capabilities within the network. It will take years, however, for the visions of the “self-defending” network to come near fruition.

Each data-in-motion encryption solution has its own strengths and weaknesses. For instance, while server-based encryption and security solutions embed security deep within the network, many of these solutions tend to be complex and more difficult to manage. They also require a significant investment in time and resources to configure and manage both network and security settings. While multi-purpose appliances are easier to install and manage, the functionality and quality of each security function—VPN, IDS, IPS, anti-virus, etc. may not provide the “best-of-breed” standard many organizations still prefer. Many vendors of such suites have also failed to adequately integrate the various security technologies to offer management features across functionality.

Security managers must evaluate the risks against their information as it travels throughout their internal network and to the networks of their external partners, and decide which approach is best, based on their resources to design an adequate data-in-transit encryption solution for their environment.

Summary

The complexity of today's business-technology systems, the sorry state of software application security, the general lack of employee IT-security awareness, and the growing “connectedness” of partners, customers, and contractors all work against the task of security managers to protect critical business information. All it takes is a single break in security anywhere in the chain for risk to reach an unacceptable level. It could be an employee who falls prey to a social-engineering attack and discloses his or her username and password to a criminal; or a package-delivery company that misplaces unencrypted backups containing customers' financial information. It could be a single unpatched server or a misconfiguration of system/network equipment for any organization to be faced with the unthinkable: having to inform thousands of customers that they're at-risk of identity theft, or tell shareholders that proprietary product research and development information was leaked to competitors.

That's why it's so crucial that senior management instills how critical information security is to the health and reputation of their organization and ensure its strategic alignment with business policy. And that's why security teams employ the effective use of several security technologies working in tandem to ensure no single point-of-failure would result in a security breach. Because it's nearly impossible for organizations to protect every facet of their network, they need to place special attention to the security of their most sensitive data-information that if compromised, could result in the loss of a competitive advantage, regulatory penalty, or even serious damage to their brand or reputation. To secure their most critical intellectual property and customer information, organizations need to create a highly-secure place on their network. An area where the strictest levels of authentication, access control, encryption, and auditing capability

All it takes is a single break in security anywhere in the chain for risk to reach an unacceptable level.

To secure their most critical intellectual property and customer information, organizations need to create a highly-secure place on their network.

ensures the highest level of security possible—at all times.

This is the very essence of the Vaulting Technology provided by Cyber-Ark Software Inc. Cyber-Ark's Vaulting Technology makes certain that an inevitable slip in an organization's security posture won't result in stolen intellectual property, or having to inform customers that they're at risk of identity theft because their personally identifiable financial information had been compromised.

Cyber-Ark's Vaulting Technology

Using the metaphor of a physical vault, Cyber-Ark developed its Vaulting Technology to create information "safe havens." Vaulting Technology protects critical information with built-in security policies and multiple-layers of tightly integrated security defenses. Cyber-Ark's Vaulting Technology is installed on a dedicated, security-hardened server. The layers of security provided include granular security-policy enforcement, firewall, session encryption, authentication, file-access control, content inspection, secured backup, file version control, and data encryption. The system runs completely independent of, and isolated from, other network and system resources, so a slip in security on the general network won't place Vaulted information at risk.

Cyber-Ark's Vaulting Technology makes certain that an inevitable slip in an organization's security posture won't result in stolen intellectual property, or having to inform customers that they're at risk of identity theft because their personally identifiable financial information had been compromised.

Vaulting Technology Overview:

Isolated Firewall & Data - Only Cyber-Ark's Vault Protocol is permitted to communicate in and out of the Vault. This ensures total control over stored information. Information within the vault cannot be altered or executed. Further layers of security are built on top of this ultra-secure environment.

Authentication - Vaulting technology requires each connection to be properly authenticated. Organizations can use passwords, security tokens, or digital certificates with Cyber-Ark's two-way challenge-and-response authentication protocol to validate each session.

Access Control - Each user accesses the Vault on a "need-to-know" basis. The Vault can be segmented into "safes"—similar to safe-deposit boxes in a typical bank vault - but, unlike physical vaults, users can see and access only the safes they are authorized to. The Vault's Single Data Access Channel eliminates any potential "backdoor" entrances to unauthorized safes.

Session & Data Encryption - For each authentication, the Vault creates an encrypted session, where every transaction and server response is encrypted. Files are encrypted both when they're stored inside the vault and during transmission. The symmetric encryption method provides internal key management. And a unique encryption key is created for each specific version of a file. Vaulting Technology provides electronically signed files that ensure data integrity during both retrieval and storage. During file access, the only encryption keys that are exposed are those required to access those specific files. The Vaulting Technology key management hides the encryption process from the user and creates no administrative burden.

Content Inspection - Vaulting Technology is capable of stripping dangerous active-code from files, such as Visual basic scripts, macros, and executable files. This technique ensures that files that are shared and stored within the Vault are free of malicious codes such as worms, viruses, and spyware.

Secure Backup and Version Control - All data stored within the Vault is encrypted, including backup versions of files. By using Vaulting Technology organizations can back up data without the concern and risk of data breach or corruption due to a security problem in the backup technology or process. When files are placed inside the Vault, the system always creates a new version that never overwrites existing files. This provides a powerful version-control mechanism that protects against both deliberate and unintentional data corruption.

Visual Security - Vaulting Technology provides inherent file audit capabilities. Every action conducted on files is fully visible to several users within an organization. Files within the Vault are marked blue, red, and green, indicating when a user accesses, updates, or inserts a file within the safe. Since these auditing trails are created and managed within the Vault, there is no way users can hide their handling of files.

Manual Security - What Cyber-Ark refers to as “Manual Security” provides a way for organizations to create and enforce powerful security policies around Vaulted information. Organizations can designate that certain files can only be accessed with “Dual Control,” which means two users must confirm the access to a safe. For example, if a researcher is attempting to access highly sensitive clinical trial data stored within a safe, her supervisor may be required to confirm access. Only after the safe receives confirmation will access be granted.

Another Manual Security feature is the Delay function, which enables organizations to stipulate that access to certain files won't be granted to certain users for a certain period of time. Organizations can also limit access to stored files with the time limitation feature. With this feature all file access could be turned off during weeknights, weekends, and holidays, for example.

Geographical Security - Vaulting technology also makes it possible to add additional security to information based on the context of the location of the user trying to access the files. For instance, forensic security reports can only be accessed from the offices of the IT security managers.

Cyber-Ark provides a number of products and solutions based on its Vaulting Technology.

Network Vault

Cyber-Ark's Network Vault, by incorporating layered security protection provided by its integrated firewall, authentication, access control, session and data encryption, content inspection, secure backup, version control, and other granular security controls, creates an ultra-secure location for organizations to protect their most critical information: product designs, customer financial (credit cards, etc.) and regulated information, HR and M&A information, and administrator/system passwords—even as they're transmitted across the enterprise network. While it could only take a single lapse in security on the organization's general network for a devious insider or other attacker to take advantage, files and information stored within and accessed from the Vault remain safe. Network Vault provides a dedicated, isolated, and secure server to store an organization's most critical information.

Inter-Business Vault

Cyber-Ark's Inter-Business Vault provides the same security functions as its Network Vault, but across a secure Wide Area Network (WAN) so organizations can securely collaborate with their extended-enterprise: partners, customers, and contractors.

Inter-Business Vault provides distributed administration of data, so distributed enterprises and those authorized can securely manage information across the Internet. With its distributed authentication capability, users at remote locations or those accessing the Vault from the networks of partners, customers, and contractors can be authenticated with their network sign-on. Inter-Business Vault can be accessed via a web client (HTTPs), and Connectors for CIFS, FTP, and SMTP for transparent LAN access. Custom integrations are created with Cyber-Ark's software development toolkit.

About Cyber-Ark

Cyber-Ark Software is the leader in Vaulting solutions for securely connecting enterprises. The Company's Inter-Business Vault enables the creation of secure instant wide area networks (WANs) for connecting enterprises with partners, customers and sub-contractors over the Internet—enabling them to exchange information as if they have deployed a shared WAN, but without actually doing so. Cyber-Ark's leading Inter-Business Vault applications include solutions for Treasury Management files, Product Design files, and Source Code. In addition to its business-to-business solutions, Cyber-Ark's Network Vault provides solutions for securely managing critical information, such as administrative passwords and critical documents, within the enterprise. Today Cyber-Ark enjoys strong customer relationships with more than 150 Global 1000 companies around the world.

Founded by a group of leading military security experts and computer engineers, Cyber-Ark Software is privately held and backed by some of the world's most successful venture capitalists, including Jerusalem Venture Partners, Seed Capital Partners (a SOFTBANK Affiliate), JP Morgan/Chase Partners and Vertex Management.

The Company is located in Dedham, Mass. and on the World Wide Web at www.cyber-ark.com

George Hulme Bio

George V. Hulme is an internationally recognized information security journalist. For more than 20 years Hulme has written about business, technology, and IT security topics. From March 2000 through March 2005, as senior editor at InformationWeek magazine, he covered the IT security and homeland security beats. His work has appeared in CNN.com, Government Computer News, Nation's Business, Network World, San Francisco Examiner, The Industry Standard, VARBusiness, and dozens of other technology publications.

This white paper was commissioned by Cyber-Ark® Software, Inc. All content and assertions are the independent work and opinions of George V. Hulme.