Data Leakage: Four Sources of Abuse

Table of Contents
Introduction .......................................................................................................................... 2
Data Leakage Is More than Regulatory Compliance ...................................................... 2
Defending the Perimeter ................................................................................................. 3
Malicious Abuse .............................................................................................................. 5
Honest Mistakes ............................................................................................................... 6
Right Action, Wrong Policy ............................................................................................. 7
Secure Computing’s Best-of-Breed Portfolio ................................................................. 7
Conclusion ....................................................................................................................... 10
Introduction

This paper will discuss the issues surrounding the protection of key corporate assets such as intellectual property, protected trade secrets, customer information, and regulated content. There are four major threat vectors: theft by outsiders, malicious sabotage by insiders, inadvertent misuse by authorized users, and mistakes created by substandard policies. We will demonstrate how a comprehensive gateway security infrastructure will help enterprises prevent data leakage from all four threats.

Data Leakage Is More than Regulatory Compliance

While governments and industry watchdog groups are mandating security measures over privacy, healthcare and financial data, enterprises have their own business priorities and concerns that are equally vital to their ongoing success.

Companies are complex entities that create, modify, store, and move vast amounts of data every day. Data leakage, including data loss and theft, has emerged as one of the biggest hurdles in the enterprise today.

According to IDC, several of the top issues faced by IT organizations involve threats to sensitive data:

- Unintentional employee errors
- Threats from outsiders: malware, spam, spyware, and hackers
- Data stolen by employee or business partner
- Insider sabotage


Data leakage can occur in any of the following situations:

- When hackers can penetrate the network and install Trojans, loggers, and other malware
- When employees surf to unprotected Web sites and get spyware injections
- When employees let their family members use office equipment
- When employees inadvertently post sensitive information to personal or professional blogs
- When protected content is sent between users unencrypted
- When technologies are insufficient to automatically identify a violation, and take steps to prevent the action
- When authentication databases aren’t updated and former employees retain unauthorized access
- When employees use personal Webmail accounts and open unsecured attachments
- When employees send confidential information to their personal email accounts so they can work remotely
- When “need-to-know” access policies aren’t enforced
- When “least privilege” policies aren’t enforced
- When corporate compliance and protection policies aren’t enforced with international partners, employees and/or third-party agents
- When employees aren’t training and consistently reminded of security policies
• When companies consider compliance as a project instead of a corporate lifestyle
• When no reporting system exists to identify violations

All of these threats can be consolidated into four major areas of concern:

1. Outsiders penetrating the network and gaining access to protected information
2. Intentional misuse by disgruntled or malicious insiders
3. Inadvertent mistakes by under-informed insiders
4. Employees following flawed policies and/or procedures

Defending the Perimeter

Every technology has a lifecycle. In the world of hacking, the “users” have moved beyond bored teenagers and are now dominated by cyber-criminals. They are using zombies, Trojans, logic bombs, scavenging, and viruses to infiltrate networks in order to gain access to sensitive information… information that they can use for profit, sabotage, or even revenge. Today’s exploits are well hidden, often dormant for long periods of time, activated only in short, virtually undetectable bursts and embedded deep into systems and resources.

Hackers can obtain protected data any number of ways:

• Adding blocks of data, or interspersing data with otherwise routine code
• Encoding data to look like something else, such as an image file
• Using “Spear Phishing,” to masquerade as an employer, boss, HR official, or colleague to obtain legitimate credentials from authorized users
• Eavesdropping on keyboard strokes to uncover passwords
• Electronic piggybacking when authorized users don’t logoff after use
• Scavenging through undeleted, under-deleted, or residual data left in computers, tapes, or disks after job execution
• Using “salami” techniques to debit small amounts of assets from a large number of sources or accounts, without noticeably reducing the whole
• Exploiting overlooked trapdoors left in by programmers or created through engineering design flaws
• Inserting logic bombs that can be used to trigger an act based on any specified condition or data that may occur or be introduced
• Using asynchronous attacks to gain access to a checkpoint restart copy of a program, data, and system parameters
• Using SQL injection attacks to gain access to databases and steal data
• Exploiting holes in non-traditional technologies:
  – Protocols such as instant messaging (IM) or voice over IP (VoIP)
  – Applications such as Powerpoint, Word, and Excel
  – Multimedia programs such as RealPlayer, Quicktime, and iTunes
• Exploiting default settings in overlooked network devices such as printers and fax machines
• Seeding malware into shared peer-to-peer directories
• Injecting malware into spam emails
• Using botnets to flood a company’s network, then blackmailing them to stop the attack (London’s Metropolitan Police recently cracked an investigation of 20,000 computers that had been hijacked by one spammer; the estimate is that hackers now have the ability to launch attacks that could potentially take out large areas of the Internet itself).
Attacks in 2006 ranged from universities to government agencies to corporations. Here are just some samples of hackers at work:

**Who**: University of California at Los Angeles  
**Date**: November 2006  
**Impacted**: 800,000 current students, faculty, and a decade of previous students  
**Data Stolen**: Names, social security numbers, dates of birth, home addresses, and contact information  
**Method Used**: The highly sophisticated attack exploited a software flaw. The hacker apparently began trying to worm into the system more than a year ago but drew suspicion only after technicians investigating performance issues on the computer system noticed odd “data traffic patterns.” “We definitely do not know who it is yet,” Jim Davis, UCLA associate vice chancellor of information technology said. “All indications so far are that this is a malicious, targeted attack and well orchestrated. And the other thing that was unnerving to us was that it was orchestrated in such a way so that it covered its tracks.”

**Who**: US Department of Agriculture  
**Date**: June 2006  
**Impacted**: 26,000 employees  
**Data Stolen**: Names, addresses, Social Security numbers, employee photos, and internal building locations  
**Method Used**: This breach was the result of a computer hacker gaining unauthorized access to an Office of Operations workstation and two servers containing employee personal data

**Who**: Ohio University  
**Date**: June 2006  
**Impacted**: Approximately 7,500 subcontractors, students, and faculty  
**Data Stolen**: Names, Social Security numbers, and wages for 2,480 subcontractors of the university, and class lists containing the names and Social Security numbers of about 4,900 current and former students  
**Method Used**: There is little information as to how exactly this breach occurred, although reports seem to indicate the system that held this information was breached by a hacker. Although Ohio University did not indicate whether the hacker originated internally or from an external source, it appears as though the system and associated files have been accessed since August 2005

**Who**: Sacred Heart University  
**Date**: May 2006  
**Impacted**: 135,000 students, alumni and those who took an entrance exam  
**Data Stolen**: Names, addresses, Social Security numbers, and in 103 cases, credit card information  
**Method Used**: This data breach was the result of a hacker that installed a root kit and shut down services on the server that held or processed this personal information

**Who**: Georgia Technology Authority (GTA), an agency of the State of Georgia  
**Date**: March 2006  
**Impacted**: Approximately 575,000 members of the state’s pension plans  
**Data Stolen**: Names, addresses, Social Security numbers, and bank account numbers of members of eight different pension plans  
**Method Used**: The breach occurred because the database that this information was stored in was broken into by a hacker via a software vulnerability
Who: Atlantis Resort
Date: January 2006
Impacted: 55,000 customers
Data Stolen: Names, addresses, credit card numbers and details, Social Security numbers, driver's license numbers, and bank account data
Method Used: Details being released are limited at this point. However, the parent company, Kerzner International, acknowledges hackers broke into their database and stole the information. It is not yet known if this was the work of an employee or that of an outside hacker

(Sources: http://idtheft.about.com/od/dataandstat1/a/2006_breaches_3.htm; http://www.eweek.com/article2/0,1895,2071946,00.asp?kc=EWSWREMLP121406SWR1)

Computer crimes have changed rapidly along with the technology. As companies become evermore reliant on their computer systems, the protection of those systems becomes even more mission-critical. Ultimately, all business crimes will be computer crimes. The only sure defense is to institute strong perimeter protections that keep every possible attack from infiltrating the network.

Malicious Abuse

Employees spend a good part of their time creating valuable information for their companies: sales contacts, intellectual property, proprietary systems, etc. They often feel they have some ownership of the property and are inclined to steal part of it when they leave the company or misuse it while they are still employed. A common scenario is a salesperson taking their contact database with them to their next job.

Threats from these disgruntled or irresponsible employees are on the rise, and the greater the individual's access and knowledge to the organization's systems, the greater the threat that individual poses. The main question resulting from these internal breaches: Did the employee have a need to know or share the compromised information?

In 2005, the largest breach of banking security in the U.S. occurred in four banks in New Jersey. Altogether over 676,000 consumer accounts were involved. Nine people were indicted, including seven former employees of the four banks, none of whom were IT workers. The breach was created by the bank employees, while they were at work, manually building a database of the 676,000 accounts using names and Social Security numbers. They pulled up the account data while working inside their banks, then printed out screen captures of the information or wrote it out by hand. While they normally conducted 40 to 50 searches per day of customer bank accounts, during this period, they performed up to 500 account searches a day, looking for new data to steal. The data was then provided to a company called DRL Associates Inc., which had been set up as a front for the operation. DRL advertised itself as a deadbeat-locator service and as a collection agency, but was not properly licensed for those activities by the state. The information was then allegedly sold to more than 40 collection agencies and law firms.

Another bank theft occurred in the London branch of Sumitomo Mitsui Bank in 2005. Thieves disguised as cleaning staff nearly stole the equivalent of more than $400 million by installing programs to record keystrokes on computers that were used to handle international wire transfers of money. After analyzing user identifications and passwords recorded by the keystroke-logging programs, they used the information to make a huge money transfer to an Israeli bank, but were foiled at the last minute when police were tipped off.

A security study of 1000 respondents performed in the UK in the summer of 2006 found some surprising results:

- 37% of men believe it is acceptable to take database information and sales leads
- 49% of 16-24 year-olds do not think that workplace theft is ‘stealing’
- 73% of graduate trainees admit to office theft
- 56% believe that companies expect things ‘to go walk-about’
- 30% of workers agree that sales leads/business contacts are rightfully their property
• 65% of workers would consider taking leads/business contacts when leaving a job
• 45% of small company employees would download data to help them in a new job
• 85% are unaware of company policy regarding what cannot be removed from the office
• 60% of employees admit to having taken something from the workplace in the past

Does this behavior concern management? Apparently not:

• Only 7% of managers agreed that they had been victims of data theft
• Only 30% believe that data theft protection should be a company priority

(Source: Prefix Security Report 2006: Theft in the Workplace)

Even large, sophisticated enterprises can become victims of malicious employees. In January 2006, Honeywell International discovered that 19,000 of their current and former employees’ personnel data had been stolen, including Social Security numbers, payroll and bank account information. Honeywell is taking action against Howard Nugent of Arizona, a former employee. Officials in their court filings state that Nugent “intentionally exceeded authorized access to this information.”

Government agencies aren’t immune either. In June 2006 information on approximately 28,000 U.S. Navy personnel and their families was discovered in five spreadsheets that were posted on a civilian Web site. Information on these spreadsheets included: names, Social Security numbers, and dates of birth.

How does an enterprise defend against the malicious insider? There are no policies or procedures that are 100% effective, but limiting user access to protected content minimizes the damage that s/he can do. Companies can implement “need-to-know” and “least privilege” policies, keep sensitive data encrypted, ensure that an employee’s rights are terminated when they are, examine all outbound electronic communications for policy violations, and maintain good forensic databases.

Honest Mistakes

No one is perfect and we all make mistakes. However, in the world of electronic assets, those mistakes can have serious impacts.

Sometimes it’s a programmer who didn’t design their system for security or conducted inadequate testing:

• In September, 2006, the Berks County Sheriff’s Office (Reading, PA) reported that the personal information (including Social Security numbers) of approximately 25,000 gun permit holders was exposed on the Internet because a contractor developed a Web-based computer records program. It seems like someone forgot to tell him that it should have been an Intranet, not an Internet, site.

• In July, 2006, the town of Hampton, Virginia performed a systems upgrade. Apparently, the upgrade affected the security controls that were previously in place, and 100,000 taxpayers suddenly had their personal information available to the public.

• In August, 2006, The US Department of Education modified their online student loan information system. A software upgrade performed by a Fortune 500 IT outsourcing company resulted in personal information (names, Social Security numbers, dates of birth, addresses, telephone numbers, and student loan information, including balances) of approximately 21,000 students viewable by anyone logged in to an account.

• In August, 2006, the Victoria Police Department in Australia released 7,000 pages of sensitive information, including private information on 291 residents. The pages were emailed to an officer who had requested just his own employee file. This was after the Victoria Police Department had been issued with several non-compliance notices and ordered to tighten security.
Sometimes it’s just human error:

- In September 2006, Circuit City and Chase Card Services compromised the personal and account information of approximately 2.6 million past and current Circuit City Cardholders when a Chase Card Services employee mistakenly discarded five computer data tapes, without erasing them first.

Enterprises can be protected against honest mistakes by implementing technologies that can assist in discovery and remediation. Monitoring all outbound electronic communication protocols will identify inadvertent policy violations through email, IM, or Web activity. Automated policy enforcement can quickly turn a user error into policy compliance. Education is the key to changing employee behavior; when a violation is detected, reminding the employee of the policy is one way to prevent future mistakes.

**Right Action, Wrong Policy**

Sometimes data leakage can occur when everyone does exactly what they were supposed to do. The fault can be traced to inadequate, outdated, or substandard policies.

Here are some examples of mistakes that companies make that create a healthy environment for exploitation and data leakage:

- A policy that states that employees can work remotely, but doesn’t specify that the work should be done on company computers that are kept current on security measures, and not home workstations which may not even have a firewall
- A flexible policy that allows users to download their own software from Web sites. While this might make users happy, it can also introduce malware from unsecured sites
- A lightweight password policy that doesn’t implement strong passwords, force passwords to expire, or allows passwords to be the same as the employee uses for personal accounts
- A policy that only requires HR to purge terminated employees once a month, providing former employees continued access for several days or even weeks
- A policy that spells out company requirements for email systems, but doesn’t expand that to instant messaging, peer-to-peer, FTP, Webmail, or blogging

For example, in an effort to comply with the Freedom of Information Act, Broward County, Florida made family court and property records dating as far back as 1978 available to the public. However, the county failed to remove sensitive data for over 1 million current and former residents (Social Security numbers, driver’s license, and bank account information, dates of birth, signature images, passport numbers, and green card details) from those public records. This breach has been going on for years, and even though they became aware of it in April 2006, officials say they won’t be able to stop it until January 2007.

Developing and tracking adequate policies is an interactive process... getting feedback on what’s working and what’s not, refining the policies, educating the users, and repeating the cycle. Without a good feedback mechanism and employee education, it’s almost impossible to improve the way a company does business.

**Secure Computing’s Best-of-Breed Portfolio**

While no system can be perfect, Secure Computing has developed an extensive portfolio of gateway, identity and access security solutions that can help enterprises win the war against data leakage, from all four threats.
Outsider Threats:
- Provides the world’s strongest application proxy firewalls, with zero-tolerance for all suspicious and undesirable traffic, including packet fragmentation, spoofing, denial of service (DoS), viruses, worms, Trojans, spam, spyware, SQL injection, fraud, and more
- Provides messaging firewalls that protect against spam and malware threats carried in emails, IM, FTP, P2P, and VoIP protocols
- Provides Web protection against spyware and malware threats carried in HTTP and HTTPS protocols

Malicious Insiders:
- Provides strong two-factor authentication tokens which can be terminated automatically when an employee leaves the company
- Automatically restricts access to users with only “need-to-know” job requirements
- Automatically scans all messages, employing advanced technologies to block sensitive data before it can leave the enterprise through email, IM, FTP, Webmail, or blogging protocols
- Encrypts all sensitive information at the gateway regardless of end user actions

Honest Mistakes:
- Automatically encrypts sensitive data, even if the user forgot the policy
- Scans outbound emails and can enforce 12 unique actions automatically
- Informs users of policy violations to improve user education and minimize the likelihood of future mistakes
- Enforces access policies to ensure that users don’t get access to more information than they require to do their jobs
- Provides end-point security so that only properly configured machines are allowed access to network resources

Substandard Policies:
- Provides pre-defined lexicons, pattern matches, and policy templates to help companies get the policies right the first time
- Provides instant notifications to compliance officers of policy violations
- Supplies extensive reporting and forensic analysis capabilities that help identify where policies might need improvement

Secure Computing’s portfolio has won practically every security award imaginable, including:

- The only security appliance vendor to have achieved the pre-eminent EAL4+ Common Criteria certification for application-layer firewalls. Secure Computing firewalls have been subject to the most complete evaluation to date of any firewalls in the industry. As a result, all of the security agencies in the US federal government and almost all of the major financial institutions in the world (DoD, CIA, NSA, FBI, CitiGroup, etc.) use Secure Computing’s Network Gateway Security appliances.
• Gartner Leaders Quadrant for Email Security Boundary, 2006. In their report, Gartner mentions some of the core capabilities that differentiate vendors, including manageability, policy-based outbound content filtering, encryption, and instant messaging and Web integration. Additionally, efficient and accurate spam and virus filtering with low administration overhead remain essential to buyers. “Leaders are performing well today, have a clear vision of market direction and are actively seeking competencies to sustain their leadership position in the market.”

• SearchSecurity’s 2006 Gold Medal Winner for Email Security. “After winning users’ trust, IronMail® has won a gold medal in email security. Not only did the product come out on top, but it also received the highest overall score of all 60 finalists in our Products of the Year. The reason is clear: IronMail offers superior quality, robust performance and a comprehensive feature set wrapped into one tight appliance.”

• IDC Market Leader In Both Messaging Security And Secure Content Management. “The company developed its gateway appliance to help customers predict, identify, and solve critical email security issues with industry-leading knowledge and state-of-the-art technology. Over the years, Secure Computing has progressed its comprehensive layered approach to protecting the messaging systems of some the world’s largest enterprises. Secure Computing provides multiple, policy-based, integrated security solutions at the network edge, gateway, and desktop to reduce total administration time companies spend on managing and securing their inbound and outbound messaging infrastructures.”

• SC Magazine 2006 Readers’ Trust Awards for Best IM Security and Best Content Security Product (Webwasher® Secure Content Management Suite), Best Two-Factor Authentication (SafeWord® PremierAccess®), and Best Web Filtering (SmartFilter®). “Overall there is very little to criticize the Webwasher 1000 for. It delivers industrial strength content security measures, times them together neatly into a single, easily deployed appliance, and delivers them at a price few competitors will be able to match.”
Conclusion

According to a November, 2006 CIO Insight survey that interviewed thousands of IT executives, managing sensitive data safely is a priority, but also a challenge. Some of the more interesting findings in this survey include:

- 51% of enterprises with revenues of over $1 billion have had at least one security breach in the last 12 months
- Top five types of security breaches most commonly cited are:
  - Penetration by spyware and other malware: 55%
  - Penetration by viruses, worms, and Trojans: 53%
  - Lost or stolen equipment containing customer data: 45%
  - Attacks on the corporate Web site (denial of service): 25%
  - Stolen data or malicious attacks by employees or former employees: 23%
- 48% of financial services firms have been a target of cyber-crime
- 25% of enterprises have been targeted by organized criminals
- 21% of enterprises have been targeted by former employees
- 21% of US enterprises believe that their current infrastructure provides inadequate protection against viruses, worms, hackers, and unauthorized access
- 42% believe that infected email poses a significant security threat
- 40% believe that attacks or infiltration of the corporate network pose a significant security threat

(Source: CIO Insights: The 30 Most Important IT Trends for 2007 http://www.cioinsight.com/article2/0,1540,2061548,00.asp)

More and more, corporate assets and regulated content are created, stored, managed, and transmitted digitally. While this provides efficiencies and cost savings, it also creates opportunities for abuse, from both the outside and the inside, from criminals and from human error. A comprehensive, gateway-based, security infrastructure will help ensure that your enterprise’s protected and sensitive data is accessed and handled properly. After all, no one wants their name on the front page of the Wall St. Journal under the headline of “Another Company Fails to Protect Consumer Data” or even worse “Company Classified Information for Sale on eBay: Buy Now.”

For more information about any of Secure Computing’s products or services, please contact us or an authorized partner.