

Data Loss Prevention: The Enemy Within



ZECURION

Treats Internal Threats

Why Focus on Internal Threats?

- 59% of employees who leave or are asked to leave a company and have access to proprietary information steal company data (02/09 Ponemon Institute survey: Data Loss Risks During Downsizing)
 - 67% of respondents who stole data used the stolen information to leverage a new job
 - The stolen information consisted of customer data, email lists, contact lists, employee records, financial reports, confidential business documents, software and other intellectual property
- Insiders are the number one cause of all data breaches, with hackers ranking a distant 5th (06/08 Ponemon Institute: 2008 Study on the Uncertainty of Data Breach Detection)

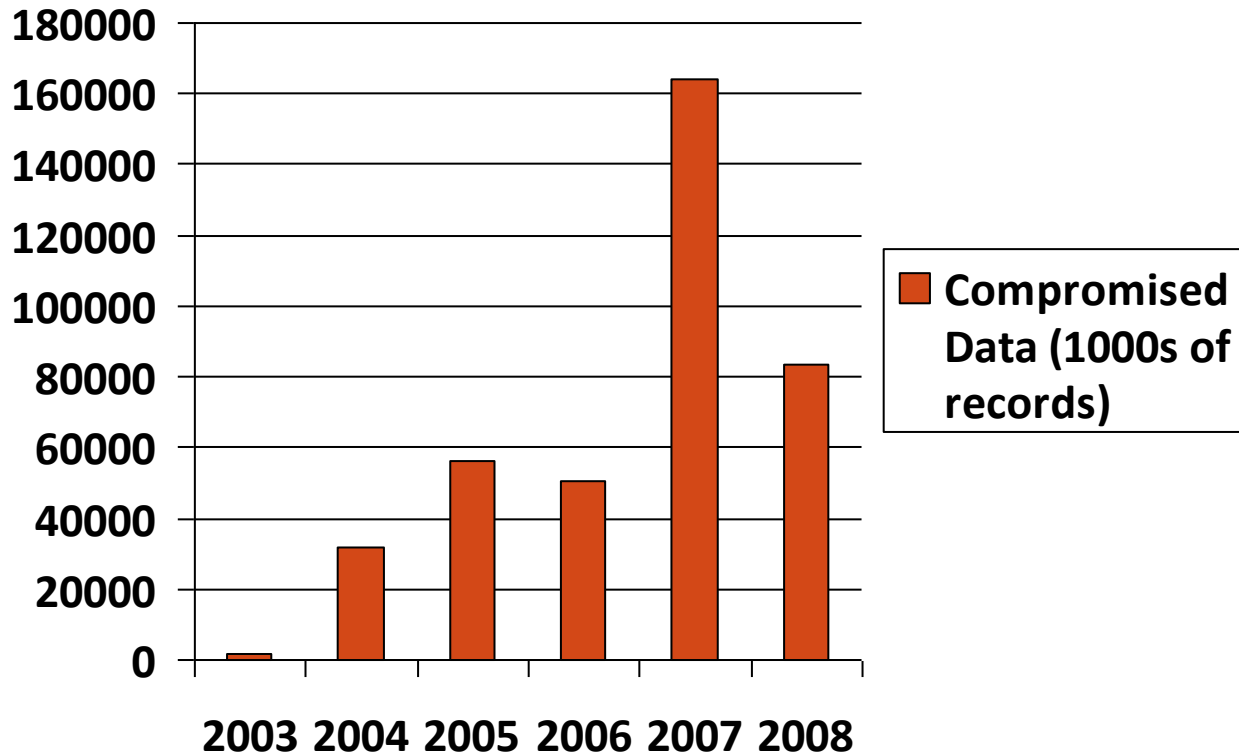
Security Breaches

- In 2008, a senior financial analyst at Countrywide was arrested for stealing customer data. According to FBI affidavits, he would download 20,000 customer profiles per week over a 2 year period to a USB drive.
- In April, 2009, Starwood Hotels files a lawsuit against Hilton alleging that former employees stole over 100,000 electronic files of proprietary and highly confidential information. They learned about the theft when Hilton returned hard drives, zip drives and thumb drives after receiving an order to preserve data related to a non-solicitation agreement with Starwood's former employees.

Security Breaches

- In 2006, a laptop was stolen from the residence of a US Department of Veterans Affairs staff member. It contained millions of names, birth dates and social security numbers of veterans and active-duty personnel. The VA pays \$20 million in 2009 to settle the class action lawsuit, even though the laptop was recovered and authorities do not believe the data was used for identity theft purposes.
- In 2008, BNY Mellon reported 2 separate instances of backup tapes being lost on their way to an offsite storage facility. Combined, the two incidences exposed data on 4.5 million people and 747 companies.

A Growing Problem



And by 2008...

- Total records compromised:
 - 83,490,075*
- Nearly a 225% increase in 8 years
- Estimated cost to the economy:
 - *\$16,864,995,150**

How Much is Your Data Worth?

- Average cost of a data breach in 2008:
 - \$202 per record
- Average total cost per breach event:
 - \$6.6 million (up from \$4.7 million in 2006)
- Pepperdine University's Graziadio School of Business and Management estimates that ensuing network downtime caused by data leakage can range anywhere from \$50,000 - \$1,000,000 per hour depending on the size and operational deployment of the network.

In Bad Company – Case Studies in Damages



GE Money
UNITED STATES



defence



MARINES
THE FEW. THE PROUD.



IRON MOUNTAIN®

HARVARD UNIVERSITY

JPMORGAN CHASE & CO.

kraft foods
Make today delicious

Georgetown
UNIVERSITY
est. 1789

GS Caltex

In 2008 alone more than 83 million records were compromised. Nearly 12.5 million customers and employees of the organizations above had their personal records compromised from the loss or theft of poorly secured data.

An Urgent Need

- Regulation is driving the need
 - HIPPA
 - Sarbanes Oxley
 - Data Protection Act (UK)
 - Massachusetts / Nevada Personal Data Protection Laws
- 44 states, along with the District of Columbia, Puerto Rico and the Virgin Islands, require that individuals be notified if their confidential or personal data has been lost, stolen or compromised
- When a regulatory breach occurs, organizations must notify all affected individuals, attempt to minimize downstream brand consequences and put solutions in place to prevent a recurrence

What Can You Do?

- Define strong access control policies that define who has access to what data and under what circumstances
- Educate your employees
- Take control of your peripheral devices
- Protect laptop hard drives
- Protect network storage and backup tapes
- Take control of your emails

Take Control of Your Peripherals

- Implement software based control of peripherals (MS Vista or 3rd Party). To be effective, make sure it has the following features:
 - Ability to define policies around access that can cover broad categories of devices (printers, USB drives, etc..) as well as users (people with read only access, super users, etc...)
 - Fine grained control that allows administrators to grant access at specific times of the day or for specific devices
 - Exception based processing which allows administrators to grant limited, restricted exceptions to the policies quickly and easily
 - Remote system management, so the solution can be administered and deployed centrally
 - Logs and shadowcopy, so that in a data loss event, there is a way to easily determine exactly what was removed and when

Protect Laptop Hard Drives

- Password based protection is not enough. The data can still be accessed.
- File and Folder Encryption is the minimum that should be enabled.
 - Supported through Windows
 - Has limitations
- Full Disk Encryption
 - Supported through Vista on the Operating System Volume
 - Supported through 3rd party software
- Whatever encryption method is chosen, make sure it supports the concept of a super-user that allows decryption by a trusted authority when the employee leaves the company

Protect Network Storage and Backup Tapes

- Encryption must be seamless and invisible to users
- Encryption Appliances:
 - Expensive, out of the budget for most small to mid-size companies
 - Built in bottleneck for accessing encrypted devices
- Software Based Encryption:
 - Cheaper to implement
 - Make sure that it has some key features to make it practical:
 - Multi-threaded encryption to overcome performance limitations compared to using an appliance.
 - Key quorum concept to avoid leaving control in the hands of a single administrator and the “Hit by a Bus” scenario
 - Centralized Administration
 - Limited to no downtime during initial encryption process

Take Control of Your Emails

- Implement controls so that you can prevent confidential information from being emailed out of your company.
- Key features to look for:
 - Fine grained control, so that authorized users can send out confidential information required by their job function, while other users are blocked
 - Ability to scan attachments with the most commonly used file types, including compressed files
 - Sophisticated content analysis to capture variations on restricted words
 - Support for a quarantine process that allows administrators to clear messages that require special handling

Summary: Realities of Securing Data

- No company is immune, regardless of size
- Theft and loss will likely continue to rise
- Requires multiple levels of protection
- Being inside the “fort” is not enough
- Small form factor mass storage = single point of failure
- Major reasons for security include:
 - Protect integrity of data, Intellectual Property and proprietary information
 - Protect against liability (SOX)
 - Protect corporate reputation and future sales