



Data Loss Prevention (DLP): The Enemy Within



ZECURION

Treats Internal Threats

Why Focus on Internal Risks?

- Drivers (What's going on “Out There?”)
 - Regulations
 - Economy
 - Common Sense
- Research shows that many organizations have done an adequate job of securing their organizations from outside intrusions, but most of these same organizations have not leveraged their resources to focus on the internal processes to protect data leakage.

Why Focus on Internal Risks?

- Some Interesting Facts
 - **Insiders are the number one cause** of all data breaches, with hackers ranking a distant 5th
 - Among companies reporting **serious data leaks, 69 percent** attribute their data security breaches to **malicious employee** activities or **employee error**
 - 59 percent 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

Some Examples of Security Breaches

- In 2008, a senior financial analyst was arrested for stealing customer data. According to FBI affidavits, over a 2 year period he would download 20,000 customer profiles per week to a USB drive.
- In 2009, a hotel files a lawsuit against another hotel alleging that former employees stole over 100,000 electronic files of proprietary and highly confidential information.
- Washington DC — “...*State Superintendent of Education staff member **accidentally** attached a **spreadsheet with students’ names, addresses and soc. sec. numbers** **to an email** ...that was then sent to students.”*
- Albany — “A former state tax department employee **with access to** various tax documents and returns pleaded guilty to illegally possessing sensitive personal data and using some of that information in an elaborate identity theft scheme.”

Some Examples of Security Breaches

- In 2006, a laptop was stolen from the residence of a U.S. 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, a major financial institution reported 2 separate instances of backup tapes being lost on their way to an offsite storage facility. Combined, the two incidents exposed data on 4.5 million people and 747 companies.
- Ghana, Africa – “...journalists investigating global electronic waste business **bought a computer hard drive in a back street market containing sensitive documents belonging to U.S. government contractor Northrop Grumman.**”

Bottom Line

#1 problem is
the #7 deployed
defense

Deployed Technology	2008
Anti- Virus	97%
Firewall	94%
VPN	85%
Com Encrypt	71%
Intrusion	69%
Vulnerability & Patch Management	65%
Data/File Encryption	53%

An Urgent Need

- Regulation is driving the need
 - HIPPA
 - Sarbanes Oxley
 - Massachusetts/Nevada Personal Data Protection Laws
 - PCI
- 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?

- *Bad News:* Can't afford to protect everything
- *Good News:* You don't have to

What Can You Do?

- Data
 - Know the value of your data
 - Know where and how it's stored
 - Know who has access
- Network
 - Monitor and control data leaving your network
- End-Point
 - Monitor and control data on the laptop and desktop
- Educate your employees (training and awareness)
- Take control of your peripheral devices

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
 - Multithreaded 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



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

Take Control of Your Peripherals

- Implement software-based control of peripherals. 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 shadow copy, so that in a data loss event, there is a way to easily determine exactly what was removed and when

What We Did

- CEO has strong understanding of technology and risks associated with data loss
- Strong internal IT audit team
- Process
 - Laptop encryption
 - Peripheral devices lockdown with USB encryption
 - E-mail encryption
 - Server hard drive and tape encryption



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
- Major reasons for security include:
 - Protect integrity of data, intellectual property and proprietary information
 - Protect against liability and regulations (SOX)
 - Protect corporate reputation and future sales



Summary: Realities of Securing Data

- Design intelligently – based on a risk assessment
- Remember: Security is not a disabler

