Data Leak Prevention
Don’t Miss the Big Picture

Victor Lee
Director, Data Protection
Trend Micro, Inc.
Why Should You Care…

- **Cost:** $6.3M per breach*
- **Loss of customers/business**
- **Brand damage**
- **Stock price decrease**
- **Regulatory fines**
- **Legal defense**
- **Notification and compensation**
- **Public relations & security response**

*Ponemon Institute, 2007
Data Loss Threats

**Stolen Devices**

Personal data on about **26.5 million** U.S. military veterans was stolen from the residence of a Department of Veterans Affairs data analyst who improperly took the material home. The data included names, Social Security numbers and dates of birth for the veterans, Nicholson said, but "there is no indication at this time" that the data had been used for identify theft.

**Data Stealing Malware**

Malware cited in supermarket data breach

By JERRY HARKAVY, Associated Press Writer
Fri Mar 28, 1:13 PM ET

Unauthorized software that was secretly installed on servers in Hannaford Bros. Co.'s supermarkets across the Northeast and in Florida enabled the massive data breach that compromised up to 4.2 million credit and debit cards, the company said Friday.

The Scarborough, Maine-based grocer confirmed a report in The Boston Globe that it told Massachusetts regulators this week about the link between the breach and the illicit programs, known as "malware."

The company doesn't know how the malware — short for malicious software — got onto nearly all its 271 stores' servers, Hannaford spokeswoman Carol Eleazer said.

**Hackers**

Security

February 21, 2007
Security Woes Snowball For TJ Maxx
By David Needle

TJ Maxx's [Quote] January report of a database breach exposing customers' financial information was bad enough.

It seems the damage, which led some customers to cancel or change their credit and debit card numbers, was worse than originally reported.
Where Do Threats Come From

Careless Insider
VP Sales of financial services company sends client list to sales team over unsecured, wireless network at airport

63% of data leaks are caused by internal employee mistakes or carelessness
IDG Mid Market (100-5000 employees) Data Leak Survey, Feb. 2008

How is Threat Realized

- Mistypes email address and customer data sent to wrong recipient or distribution list
- Transmission intercepted over unsecured network

Result
- Privacy violations
- Regulatory Violations
- Customer Churn
- Client Notification Costs (~ $100/record)
Where Do Threats Come From

Malicious Insider
Disgruntled auto designer prints or copies CAD files

78% of data breaches come from authorized insiders
Ponemon Institute, 2006 research study

How is Threat Realized

- Intellectual property sent/sold to competitor
- Patent infringement suits
- Impact on technology leadership
- Loss of Business
- Lower stock price
Did You Know....

• Nearly 50% of respondents admitted to sending confidential information by public Web mail

• 32% of respondents admitted to sending confidential information by public IM

• Over 30% of respondents downloaded an executable file to their corporate laptop while they were off of the corporate network

• In the US, of those who admitted to taking more chances with their work PC then their home PC:
  – 36% did so because they had an IT person to support them if something bad happened
  – 20% did so because it's not their computer

\[\textbf{It only takes one}....\]

Economic Events Increase the Risk

Big Three want more money in loan

The price tag of a loan to the Detroit automakers could top $3 billion, up to $188 billion for Ford, $9 billion for Chrysler, $7 billion.

By Chris Isidore, CNNMoney.com senior writer

Unemployment tops 6% for first time in five years

August’s jobless rate jumps to 6.4% from 5.9% in July, the Labor Department reports. The manufacturing sector is among the hardest hit.

By Maura Reynolds

The Recession Is Made Official

Stocks Take a Dive

The Recession Is Made Official

By John C.卧

HSBC, Credit Suisse Swing the Axe

As financial crisis bites deeper, the two big banks are both trimming workforces in Britain. A trade union reacted with fury.

By Sarah Farrell

The Independent

Another 1,150 redundancies in Britain's banking industry were announced yesterday, as Credit Suisse cut 10% of its UK workforce and HSBC said it was axing 500 jobs.

The Independent
Market Evolution of Content Filtering & DLP

• The Early Days…
  – Basic outbound email filtering at the Gateway

• Entrance of Network DLP
  – Multi channel monitoring using more advanced techniques

• Data Discovery and Classification
  – The ability to discover and classify sensitive data at rest within the enterprise, wherever it may be stored (i.e. File shares, DB, DMS, etc.)

• Endpoint
  – Successful blocking of all channels at the endpoint (i.e. USB, CD/DVD, Webmail, Email, Printing, etc)
  – Unified policies on and off the network
DLP Best Practices

Understand Business Objectives

Develop a proper framework of standardized controls

Properly Set Expectations

Phased Implementation

Requires a combination of people, processes and technology

CIO Mandate

Protect my data but don’t interfere with the business
DLP Must Haves…

- Optimized Endpoint Fingerprinting
- Full and Partial Fingerprint Matching
- Discovery of Data at Rest
- Real-Time Content Scanning of Sensitive Data
- Smart Identifiers (i.e. SSN, DOB, Bank Account Numbers)
- Regulatory Compliance Templates
- Language Independence
- Online/Offline Policies
- Device Control
- Centralized management
Case Study: Associated Fuel Pump Systems Corporation (AFCO)
Case Study

- Associated Fuel Pump Systems Corporation (AFCO)
- Established in November 1989, Anderson, South Carolina
- Multinational joint venture between Robert Bosch GmbH of Germany and DENSO International America
- Focus on manufacture of high pressure, turbine-type electric fuel pump
- A sample customer list includes Chrysler, Ford, GM, Honda, Toyota
AFCO Data Security Initiative

Business Drivers
- Comprehensive data security policy from parent companies
- Protect customer data and intellectual property
- Summer intern caught stealing
- Do more with less

Project Scope
- Block data from leaving the NW
- Online/Offline protection
- Phase 1 – Monitor only to help increase understanding
- Phase 2 – Tighten rules where needed

Technical Requirements
- Granular filtering off-network
- Support for USB, CD/DVD, Webmail, Email, Wireless
- True content scanning in real time (not device control on/off)
- Centralized Management

Results
- Deployed on time & on budget
- After only 3 weeks, areas to further tighten security
- Visibility into employees compliance with new security policies
- Very short ROI
Thank You