Crime and Carelessness

Gaps that enable the theft of your most sensitive data

Ryan Boudreau – Canadian Data Loss and Compliance Specialist
Symantec™ Global Intelligence Network
Identifies more threats, takes action faster & prevents impact

Rapid Detection

**Attack Activity**
- 240,000 sensors
- 200+ countries

**Malware Intelligence**
- 130M client, server, gateways monitored
- Global coverage

**Vulnerabilities**
- 32,000+ vulnerabilities
- 11,000 vendors
- 72,000 technologies

**Spam/Phishing**
- 2.5M decoy accounts
- 8B+ email messages/day
- 1B+ web requests/day

**Worldwide Coverage**, **Global Scope and Scale**, **24x7 Event Logging**

Preemptive Security Alerts, Information Protection, Threat Triggered Actions

Copyright © 2009 Symantec Corporation. All rights reserved.
Sources of a Breach

Organized Criminal
Well Meaning Insider
Malicious Insider
Anatomy of a Breach

- Incursion
- Discovery
- Capture
- Exfiltration
192% growth in spam from 2007 to 2008

In 2008, Symantec documented 5,471 vulnerabilities, 80% of which were easily exploitable

90% of incidents would not have happened if systems had been patched

In 2008 we found 75,000 active bot-infected computers per day, up 31% from 2007
91% of records compromised in 2008 involved organized crime targeting corporate information

81% of attacked companies were non-compliant in PCI

67% of breaches were aided by insider negligence
285 million records were stolen in 2008, compared to 230 million between 2004 and 2007

Credit card detail accounts for 32% of all goods advertised on underground economy servers

IP theft costs companies $600 billion globally
Security Market Drivers

Exfiltration

“Gov’t Posts Sensitive List Of US Nuclear Sites”  Associated Press

“Goldman May Lose Millions From Ex-Worker’s Code Theft”  July 7 (Bloomberg), Goldman Sachs

“2 Men Accused Of Swiping CC Numbers”  July 2 (Bloomberg), KPHO.com

“Royal Air Force Embarrassed By Yet Another Sensitive Data Loss”  May 25, UK News
1

Poorly Protected Infrastructure
Lack of IT Policies
3

Poorly Protected Information
Poorly Managed Systems
Protect the Information

Symantec™
Data Loss Prevention Suite
Symantec™
Data Loss
Prevention Suite

- Discover where sensitive information resides
- Monitor how data is being used
- Protect sensitive information from loss
Mission statement of traditional security

**Mission**: Deploy countermeasures to protect the containers of crucial assets

Assets

- DRM + Encryption
- Anti-malware
- Perimeter security

Threats
So what’s wrong with this picture?

Today’s threat landscape is massively more complex and diverse than the infoscape battlefield we have been trained to defend.

Traditional infosec seeks to protect the containers of crucial assets and largely ignores protection of the data itself.

Perimeter security...
Data Loss Prevention answers these three crucial questions:

1. Where is your confidential data?
2. How is it being used?
3. How best to prevent its loss?
Key DLP Requirements

**DISCOVER**
- Find data wherever it is stored
- Create inventory of sensitive data
- Manage data clean up

**MONITOR**
- Understand how data is being used
- Understand content and context
- Gain enterprise-wide visibility

**PROTECT**
- Gain visibility into policy violations
- Proactively secure data
- Prevent confidential data loss

**MANAGE**
- Define unified policy across enterprise
- Remediate and report on incidents
- Detect content accurately
Key DLP Requirements

**DISCOVER**
- Find data wherever it is stored
- Create inventory of sensitive data
- Manage data clean up

**MONITOR**
- Understand how data is being used
- Understand content and context
- Gain enterprise-wide visibility

**PROTECT**
- Gain visibility into policy violations
- Proactively secure data
- Prevent confidential data loss

**MANAGE**
- Define unified policy across enterprise
- Remediate and report on incidents
- Detect content accurately
How to Stop Data Breaches

- Protect information proactively
- Automate review of entitlements
- Identify threats in real time
- Integrate security operations
- Prevent data exfiltration
- Stop targeted attacks
In Conclusion

• Threat agents behind breach
  – Hackers
  – Well-meaning insiders
  – Malicious insiders

• Primary risk factors leading to breach
  – Extensive internal exposure of confidential data
  – Failure to identify theft from malicious insiders
  – Poor protection against exfiltration of confidential data

• How do I know if I am at risk? Answer these questions
  – Do I know if there are signs of incursion into my perimeter?
  – Where is my data? Where is it going?
  – What are my biggest points of exposure of crucial data?