



Protect what you value.

Your Data is Your Life

March 2009

© 2009 McAfee, Inc.

Agenda

- The Problem: Data is Lost or Stolen Everyday!
- Securing Data Requires Different Thinking
- McAfee's Data Protection Solution

 Introducing Total Protection for Data (ToPS Data)
- Summary







The Problem

Data is Lost or Stolen Everyday!

Data Loss: Next Inevitable Corporate Disaster?



Data Protection: #1 CISO Priority Today

Merrill Lynch

2007 CISO Survey



Increasing Need for Mobile Access to Data

Explosive Growth in Mobile Devices

- Information and data moving out of corporate perimeter
- Storage capacity grows as devices become smaller
- Advances in mobile device technology will continue to produce new and more powerful devices

McAfee





Increasing Regulatory Pressure

- Growing in number and complexity
- Public disclosure is required in the event of data loss
- Intellectual property loss and theft is also a concern

McAfee[•]





Increasing Regulatory Pressure



Source: Google Maps International Crypto Law.



Increasing Regulatory Pressure





Florida

Florida Unlawful Use of Personal Identification Information Act

- (HB 481) requires businesses to notify individuals when a security breach results in their personal information being released to unauthorized parties if the breach has or will likely result in harm to the affected individuals. The Act specifies the notification steps businesses must follow in the event of a security breach.
- FL acts enforce:
 - Civil or Criminal penalties for failure to notify of breach
 - Exemption for immaterial breaches
 - Exemption for public information, or during a criminal investigation





Am. Fed'n of Gov't Employees v. Hawley, D.D.C., No. 07-00855, 3/31/08.

- The Crime:
- Class action by TSA employees against the TSA itself due to discovery (on May 3rd 2007) of a hard drive "that was missing from a controlled area at ..TSA HQ". The drive contained personnel data for 100,000 individuals (payroll, SSN, bank accounts, DOB etc).

The Court:

 "rejecting argument to narrowly interpret "actual damages" to mean only pecuniary losses and following instead "the recent trend at the District Court level.. To allow Privacy Act suits seeking general compensatory damages, such as pain and suffering and non-pecuniary losses, to proceed"





Exploit	Count of records	Sum of records
LostDrive	10	18936554
Hack	78	13824216
LostTape	12	13398471
LostMedia	20	11187570
StolenTape	13	7630396
SnailMail	23	4219606
FraudSe	41	2366970
StolenLaptop	98	1576007
StolenComputer	24	1013030
Disposal_Drive	1	1000000
Web	65	890051
StolenDrive	5	98738
Unknown	22	72822
Email	18	44888
LostLaptop	4	22013
Web/StolenDocument	1	13500
Disposal_Computer	2	6900
StolenDocument	14	6127
LostDocument	9	5310
Disposal_Document	26	1761
Hack/Web	2	500
Virus	5	320
StolenMedia	2	200
Web/Unknown	1	198
StolenComputer/StolenDrive	1	6
Grand Total	503	76316154

Row Labels	Count of records	Exploit
StolenLaptop	98	1576007
Hack	78	13824216
Web	65	890051
FraudSe	41	2366970
Disposal_Document	26	1761
StolenComputer	24	1013030
SnailMail	23	4219606
Unknown	22	72822
LostMedia	20	11187570
Email	18	44888
StolenDocument	14	6127
StolenTape	13	7630396
LostTape	12	13398471
LostDrive	10	18936554
LostDocument	9	5310
Virus	5	320
StolenDrive	5	98738
LostLaptop	4	22013
StolenMedia	2	200
Hack/Web	2	500
Disposal_Computer	2	6900
Web/Unknown	1	198
Web/StolenDocument	1	13500
StolenComputer/StolenDrive	1	6
Disposal_Drive	1	1000000
Grand Total	503	76316154

Source: Datalossdb.org, last 12 months records





Foreign hacker accessed UF student, employee records

By Nathan Crabbe Sun staff Writer

Published: Thursday, February 19, 2009 at 9:51 a.m. Last Modified: Thursday, February 19, 2009 at 12:49 p.m.

A foreign hacker gained access to a University of Florida computer system containing the personal information of more than 97,200 students, faculty and staff, UF announced Thursday.

The files included the names and Social Security numbers of individuals who used UF's Grove computer system since 1996. A hacker in the Caribbean nation of Antigua and Barbuda accessed the system Dec. 22 and exploited a security hole, according to a UF police report.

An information technology staff member discovered the breach Jan. 14 during a review of computer systems. UF sent notification letters Tuesday to most individuals with information on the system, but was unable to find addresses for about 5,000 of them.

UF spokeswoman Janine Sikes said it's unknown whether the hacker accessed personal information.

"We know somebody got in a hallway, for example, but we don't know if they opened any doors with information in them," she said.

After the breach was discovered, UF shut down the Grove system. The system contained course information with Social Security numbers and at one time required users to verify





Incidents		CONT. STORE SERV COME HOU RECORD SECO RECORD HOU RELOWED SAVE S	
WEB Date: Organ	260: Social Security numb 2006-04-10 Records Lost: U nizations: Broward Co. Records	Ders and other information posted to public web site Inknown Source: Inside Accidental Submitted by: admin Location: US s Division FL	comments: 0
010101010101 ID: 1	1208: Compromised user	name and password opens access to names, SSN's, DoB's, and driver's licenses.	comments: 1
HACK Date: Organ	2008-09-19 Records Lost: 1 nizations: City of Coral Springs,	2,120 Source: Outside Submitted by: d2d Location: Coral Springs FL, US FL, ChoicePoint	
Organizations			
City of Coral Spring	gs, FL		
Incidents: 1	Records: 12,120	Headquarters Location: Coral Springs FL, US	
Broward Co. Recor	rds Division FL		
Incidents: 1	Records: 0	Headquarters Location: Fort Lauderdale FL, US	
Paymaxx Incidents: 1	Records: 100,000	Headquarters Location: Hollywood FL, US	
DHL Incidents: 2	Records: 2,010,000	Headquarters Location: Fort Lauderdale FL, US	
WellCare Incidents: 1	Records: 71,000	Headquarters Location: Tampa FL, US	
University of Miami Incidents: 1	Records: 2,100,000	Headquarters Location: FL, US	
Hillsborough Comm Incidents: 1	nunity College Records: 2,000	Headquarters Location: Tampa FL, US	
University of Florid Incidents: 1	a College of Dentistry Records: 344,482	Headquarters Location: Gainesville FL, US	
Dr James Barringe Incidents: 1	<u>r</u> Records: 0	Headquarters Location: Fort Myers FL, US	
Concrete Reinforci Incidents: 1	ng Products Records: 0	Headquarters Location: Miami FL, US	





Trends in NA regulation...

- 46 USA states, 4 Canada provinces have, or are applying data breach exposure regulation (Iowa signed up in May).
- Over 200 regulations world wide which apply protection to PII
- Many of the USA state statutes require notification requirements only for breaches in which some or all of the PII compromised was unencrypted (i.e., Rhode Island, California, Tennessee, Texas, Utah). Notification is required in New York, North Carolina and Pennsylvania for encrypted personal information if the encryption keys are compromised along with the encrypted data. Some states have defined the term "encryption" (Maine, North Dakota, Indiana), while others have not (California, Arkansas, Louisiana, Illinois).
- No breach laws in Kentucky, Mississippi, Missouri and South Dakota (yet!)





Increasing Risk of Information Theft

- 19 people a minute become new victims of identity theft due to data breaches¹
- During a 3 year period, over 217 million Americans were victims of identity theft or exposure²
- Each data breach costs an average of \$6.3 million³
- A typical Fortune 1000 company can't locate 2% of their PC's⁴
- A typical Fortune 1000 financial institution loses 1 laptop a day⁵



- Identity Theft Resource Center, 2007
 2007 Ponmon Institute Cost of Data Breach study
- 3., 4., 5. www.privacyrights.org





Understanding the Risk The Market Value of Your Sensitive Data



\$980-\$4,900 Trojan to steal account information









McAfee









The Major Threats

McAfee[•]





The Major Threats

"I've seen organizations spend hundreds of millions of dollars on security safeguards that were penetrated by a knowledgeable person with a handheld device."

> Bill Boni CSO, Motorola







Securing Data Requires Different Thinking

Today's Security Solution Gap

- Most information security products don't actually secure information
 - They protect networks and servers
 - They do little to protect the confidentiality and integrity of information
- Information is in constant motion throughout its lifecycle—making it difficult to lock down
 - Perimeters and resources are constantly being traversed

McAfee^{*}





Current Approaches to Security Do Not Protect the Most Valuable Asset: Your Data

System-centric view of data protection:

Protect the perimeter, one system at a time







Data Protection Requires Different Thinking

Data is not static, so security cannot be static – it must follow and persist with the data. This is Data-Centric Protection.







Throwing Point Tools at the Problem Doesn't Work!

\$	High Management Cost	Non-security staff must manage myriad of point security systems. Compounds with changes in personnel and systems
	No Alignment to Policy	You are unable to align needs with security policy requirements
	Life Cycle Vulnerabilities	Managing the lifecycle of security rules becomes overly complex, increasing infrastructure vulnerability
	Broken Business Processes	Businesses processes break as systems go their own way on security
Q	Data Loss Risk	Lack of centralized monitoring and auditing opens vulnerabilities that could lead to data loss





Data Protection Requires Different Thinking



Summary

- 1. There is increasing regulatory pressure to protect data
- 2. Insiders are the biggest threat to your data and they are increasingly more mobile
- 3. A breach is a breach no matter how big or how small, it puts your business at significant risk
- 4. There are 7 major threats at the endpoint to your data which ones worry you the most?
- 5. Traditional approaches to data security won't work you need data-centric security that enables your data and infrastructure to protect itself
- 6. Throwing point tools at the problem is not a sustainable solution
- 7. McAfee provides you with the comprehensive solution you need to address the risks to your data









Protect what you value.

Thank You!

© 2009 McAfee, Inc.



McAfee's Data Protection Solution

The Solution: McAfee Data Protection





McAfee is Your Trusted Advisor

Too many vendors, too many use cases, too overwhelming



Increasing Protection and Compliance





McAfee Endpoint Encryption



McAfee

You need

- Encryption for laptops, desktops, and mobile devices with the flexibility to choose full-disk or file/folder encryption
- Confidence in integrity of sensitive data when a device is lost or stolen
- Safe Harbor protection (i.e. Loss of encrypted data = non-event and does not require public disclosure)

McAfee offers

- Military-strength certified encryption algorithms
- Broad support for laptops, desktops, and mobile devices
- Full audit-trails for compliance & auditing needs
- Network-based control and "over-the-air" management
- Certifications: FIPS 140-2, Common Criteria Level 4 (highest level for software products), BITS, CSIA, etc.



McAfee Data Loss Prevention



McAfee

You need

- To prevent users from accidentally or maliciously leaking sensitive data
- Full visibility and control over usage & movement of confidential data
- To enable your infrastructure and data to protect itself

McAfee offers

- Protection against accidental leakage via everyday user tasks
- Complete spectrum of actionable responses upon detecting loss of confidential data such as
 - Detailed logging & forensic evidence gathering
 - Real-time prevention & blocking
 - User and administrator notification
 - Quarantine of confidential data



McAfee Device Control



You need

- To monitor and allow only authorized devices to connect to endpoint
- Restriction and blocking capabilities of the use of unauthorized devices such as iPods
- Enforcement control over what data can be copied onto authorized devices

McAfee offers

- Fine-grained control of data and devices
 - Only allow company-authorized devices
 - Enforce control over what data can be copied to devices
- Policies per user, group or department, i.e. allow CEO to connect any device while other employees can only connect sub-set of devices
- Detailed user and device-level logging for auditing and compliance needs



McAfee Encrypted USB



You need

- Secure external storage media for your power users
- Ability to ensure sensitive data transported via external media is continuously protected

McAfee offers

- A range of secure portable storage devices
- Strong Access Control and Encryption
- Centralized Management
- Internal and External Compliance Support





McAfee ePO: Centralized Management and Compliance Support



• You need:

- Data protection to support compliance efforts for tough global data privacy regulations
- Detailed logging and auditing for internal and regulatory compliance needs

• McAfee offers:



McAfee

- Detailed auditing and logging to meet the toughest regulations
- "Safe Harbor" protection with data encryption
- Rich set of policy & reporting templates to help comply with regulations

