Data Breaches and Encryption

Why, When, and How

Adrian Lane
Securosis, L.L.C.

Perspective ...

Dear Customer,

Egghead.com has discovered that a hacker has accessed our computer systems,
potentially including our customer databases. While there is no indication
that any customer information has been compromised, as a precautionary
measure, we have taken immediate steps to protect you by contacting the
credit card companies with whom we work. They are in the process of
alerting card issuers and banks so that they can take the necessary steps to
ensure the security of cardholders who may be affected.

We wish to underscore that we have taken these steps as precautions. We
have no information at this time to suggest that any credit card information
has been compromised. We are investigating this possibility, and we are
doing everything we can to proactively protect you. If you would like
further information, you may wish to contact the issuer of your credit card
to determine what steps they are taking. We regret any inconvenience this
may cause you.

We issued a press release on this matter earlier today. [...] If you have
additional questions, please call our customer service team at 1-800-EGGHEAD
(344-4323).

Respectfully,

Jeff Sheahan, President & CEO, Egghead.com, Inc.

Friday, 22 December, 2000

What We Learned

- Most people assumed Egghead.com went out of business due to this breach.
- Analysis of their business metrics revealed that the company was in decline due to mismanagement long before the breach.
- We learned the wrong lesson.
- It inspired a (short) generation of secrecy.

Breach Parade ...

- November, 2001: Ziff-Davis, *"Hundreds" of credit cards*
- January 2002: Experian/Ford Motor Credit Company, *13,000 full credit reports*
- January 2003: TriWest/DoD, *562,00 veteran's SSNs*
- January 2003: IBM/ISM (Canada), *180,000 records*
- June, 2003 PetCo, *500,000 credit cards*
- December, 2003: Axciom, *Over 1B email records for spam*
- March, 2003: Data Processors International: *Over 5M credit cards*

July, 2003

California SB 1386
Enacted

Securosis.com

And promptly ignored...

ChoicePoint

- The first major 1386 disclosure.
- Unusual activity detected on September 27, 2004 on 50 small business accounts.
- Fortuitous early missteps!
- 35,000 California residents notified on February 8, 2005.
- February 16 ChoicePoint reveals problem

ChoicePoint Losses

FTC Settlement	$10M
Notification Costs	$2M
Legal and Professional Fees	$9.5M
Lost Sales From Business Practice Changes	$15M-$20M
Victim Trust Fund	$5M
Shareholder Lawsuit	$10M

Securosis.com

What We Learned

- Business Policy Failure
- They experienced a similar incident in 2002.
- Technical controls cannot eliminate business policy failures, but go hand in hand.
- Taught the industry to react differently, not to secure the data

Business Perspective

- Businesses suffer from breaches even if customers don't suffer from fraud.
- Viewed as an internal issue, not external
- Silence benefitted market stability
- Fraud was acceptable ... to a limit
- Handled by PR, not Security

357,043,401

Records Lost As Of September 15, 2008

Source: Attrition.Org/OpenSecurityFoundation

Big Scary Number

- Completely irrelevant as used today
- No indication of fraud in many cases
- No indication of significant disruption to individual business operation
- No indication of slowing down
- Little indication that businesses are motivated to act differently

Big Scary Number Cont.

- Signifies a serious problem; not an individual business, rather the entire credit card system!
- Entire system may need re-engineering
- 50M compromised numbers could be used to collapse eCommerce system
- RBS Worldpay shows mass fraud is possible
- Heartland shows mass data theft is possible

The Top 4 Causes Of Data Breaches

- Lost/Stolen Laptops
- Lost/Stolen Backup Tapes
- Inadvertent Disclosure
- Hacking/Compromise

Securosis.com

Lost Laptops and Media

- Jan 3, 2004: Triwest: Stolen computer exposed 562,000 SSN's of military personnel
- May 23, 2005: MCI: laptop stole with 16,500 employee records from unlocked car
- August 30, 2005: JPMorgan Chase laptop stolen with information of premier private banking clients
- June, 2006: IRS loses nearly 500 laptops over 3.5 years
- March, 2006: Ernst & Young loses laptop with personal information of thousands of corporate customers
- June, 2006: 243,000 Hotels.com customers exposed in second incident, laptop stolen from car in February
- February, 2006: a Deloitte & Touche employee leaves a CD with

85, 839,281

From lost/stolen laptops, desktops and portable media
in 335 reported incidents

Source: Attrition.Org

Veterans Administration

- On May 22, 2006, the VA reveals that a laptop and external hard drive with 26 million records stolen.
- The VA blames an employee; Inspector General concludes management is also culpable

Securosis.com

Veterans Administration

- On May 22, 2006, the VA reveals that a laptop and external hard drive with 26 million records stolen.
- On June 23rd, OMB M-06-16 is issued requiring laptop encryption within 45 days.
  - No funding is provided.
- The laptop and drive are recovered on June 28th.
- On January 22, 2007, the VA reports a lost hard drive with 48,000 unencrypted records

HM Revenue and Customs

- October, 2007: Laptop lost with records on 2000 investors.
- Officials reveal to Parliament that 41 laptops were lost or stolen in the past 12 months.
- A CD with 15,000 Standard Life customers also lost.

Securosis.com

HM Revenue and Customs

- October 18th, 2007: A junior official mails 2 CDs with the UK's child benefits database.
- November 8th, 2007: The missing CDs are reported to senior management. Records of 25M Britons are at risk.
- Officials blamed the employee, but further investigation revealed this is a routine practice.

Securosis.com

mobile

adjective |ˈmōbəl; -ˌbēl; -ˌbīl|

able to move or be moved freely or easily

Securosis.com

What We Learned

- Laptops and portable media get lost and stolen. Even when they have sensitive data on them.
- Accept it, embrace it, and do something about it.
- Business policies are insufficient when they are manual.
- Options: Encryption

Four Rules for Encryption

1. If data moves physically or virtually
2. Any storage
3. For separation of duties
4. Regulatory mandate

Securosis.com

It Works ... provided

- Good implementation & algorithm
- Reasonably secure Key Management
- Distribution with trusted PRNG
- Good entropy
- Running on un-compromised platforms

Mobile Encryption Options

Portable Media

Whole Drive

Partial-System

*Or choose to not store it at all ...

Securosis.com

Data Encryption Options

File/Folder

Application/
Database

Media

Not a Panacea

- Need good access & authorization
- Need audit
- Reliable platform & network security
- Data Validation

Bank of America

- On February 25th, 2005 reports surface that backup tapes with 1.2M credit card records are lost.
- The tapes contained information from a credit card program for federal workers, including 60 senators.
- Tapes believed stolen by baggage handlers in December.
- Sen. Pat Leahy, D-Vt holds Congressional hearing.

Securosis.com

Lost Tapes

30,331,283 Confirmed Records Exposed

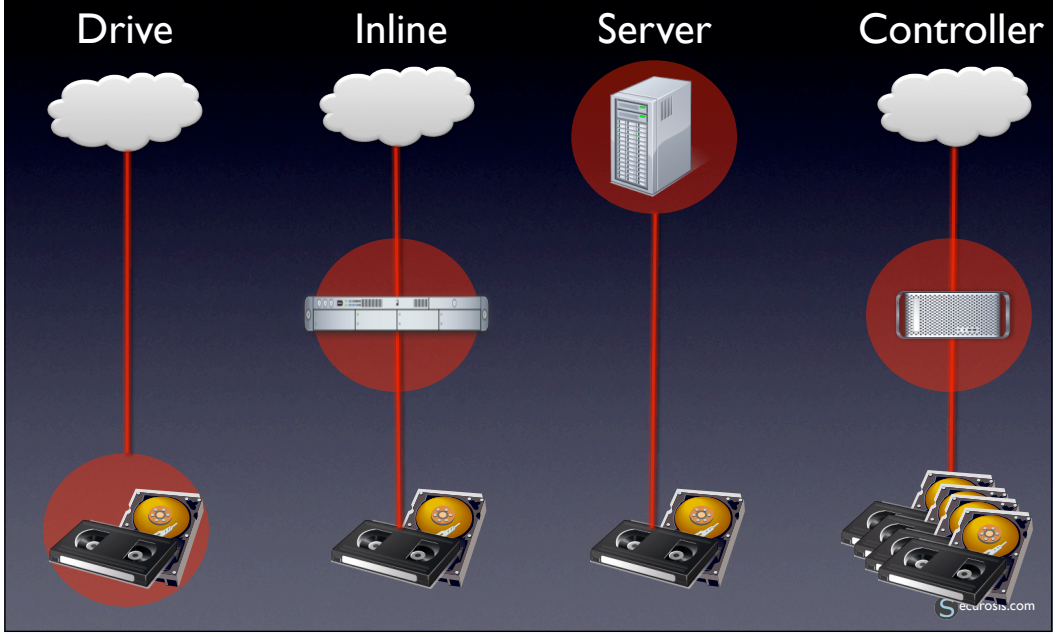
In 51 Incidents

Securosis.com

What We Learned

- Tapes must be encrypted, eliminated, or treated like cash.
- Just losing track of a tape is enough to trigger a disclosure.

Tape/SAN/NAS Encryption



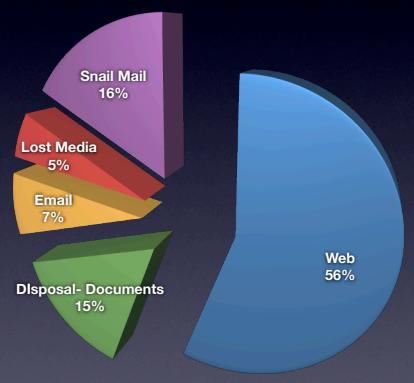
“Oops”

- The New York Times scooped a story about a $1B settlement between Eli Lilly and the US Government.
- An outside attorney with Pepper Hamilton accidentally emailed the Times reporter a detailed summary of the case, meant for another law firm.
- The breach source wasn’t discovered until after the article was released.

Securosis.com

Primary Inadvertent Disclosure Sources

Number of Incidents

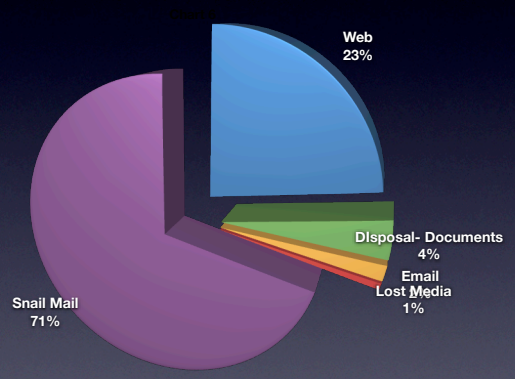


Losses labeled as 'Accidental-Internal'
Some types not included

Securosis.com

Primary Inadvertent Disclosure Sources

Records Lost



Losses labeled as 'Accidental-Internal'
Some types not included

Securosis.com

What We Learned

Accidental disclosure is just as damaging as malicious attacks, and occurs just as frequently.

Autocomplete is *not* your friend

Preventing Disclosure
DLP

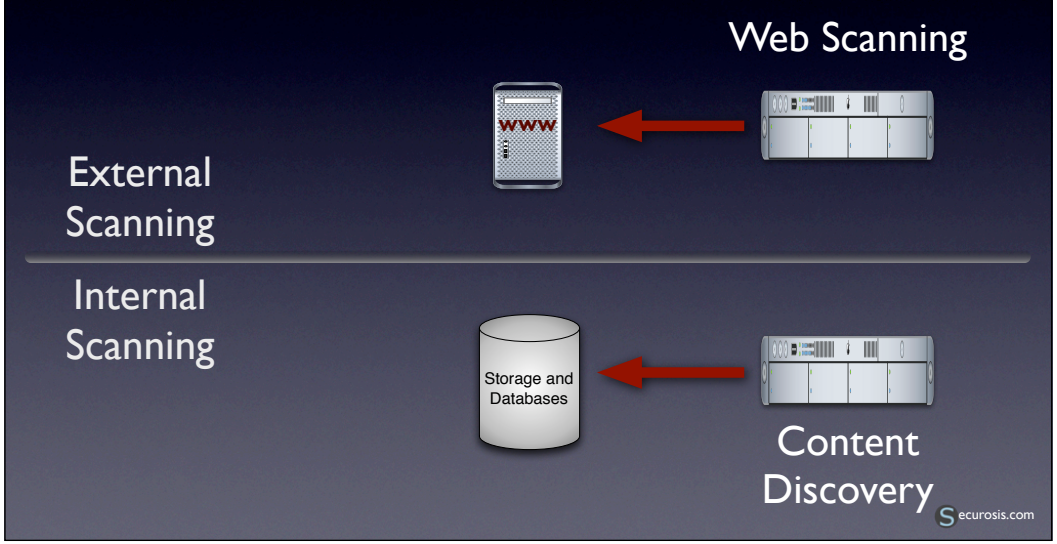
In Motion

At Rest

In Use

Securosis.com

Limiting External Exposure



A Company Destroyed

- On June 17, 2005, MasterCard states that CardSystems Solutions was breached and 40 million transactions exposed.
- The fraud was originally detected by National Australia Bank in November, 2004, and traced to CardSystems in January, 2005.
- Visa and MasterCard began investigations in April.
- On May 22, CardSystems states they discovered the breach and notified the FBI the next day.

Securosis.com

CardSystems Solutions

- CardSystems was PCI certified in June of 2004.
- During the breach investigations, it was revealed they stored track 2 data in violation of PCI.

- CardSystems was breached using a SQL injection attack through a web application.
- Code was locally installed and exported data every 4 days.

TJX

- On December 18th, 2006, TJX discovers suspicious software on their systems.
- The Secret Service begins investigating, and banks, credit card processors, and credit card companies are notified the day after Christmas.
- The breach becomes public on January 17th, 2007.

Securosis.com

45.7 Million Customers Initially Affected

Securosis.com

- TJX charged off $5M in the first 3 months after the breach for investigation and remediation.
- By August, estimated losses rose to $256M.
- Sales rose 9% over the same period the precious year, to $4.3B in the second quarter.
- The breach went back to at least 2005.

Securosis.com

- Banks are currently seeking class action status for a lawsuit to recover costs of fraud and re-issuing credit cards.
- In a court filing, fraud related charges for Visa alone range from $68M to $83M.
- Visa has fraud reports in 13 countries.

Securosis.com

http://www.msnbc.msn.com/id/21454847/
http://www.boston.com/business/globe/articles/2007/08/15/cost_of_data_breach_at_tjx_soars_to_256m/?page=2

94 Million Records Exposed

Based on the class action court filings.

How It Happened

Compromise of WEP encrypted wireless network

Compromise of in-store job application kiosks

Securosis.com

What We Learned

- Sophisticated for-profit cyberattacks are increasing at an alarming rate.
- In many cases, losses are compounded by victims keeping more data than needed.
- The less data you keep in fewer places, the less you need to secure.
- Watch your outbound data!

September 11, 2008

Losses are estimated as over
$400 Million.

Securosis.com

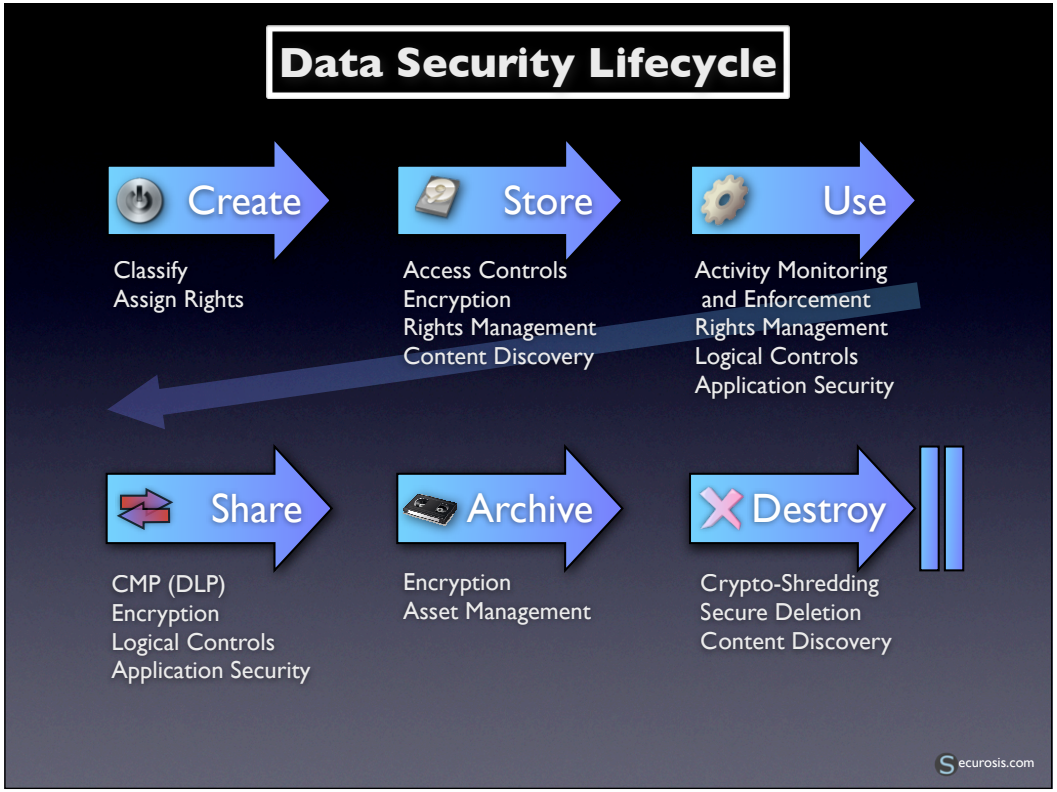
Heartland Payment Systems

- On January 20th, 2009 Heartland announced there was a breach in 2008
- Announced effort to encrypt end to end
- Contacted 150,000+ merchants
- Over 600 financial institutions effected

Securosis.com

To infinity and beyond...

Securosis.com


Data Security Lifecycle
Create
Classify
Assign Rights
Store
Access Controls
Encryption
Rights Management
Content Discovery
Use
Activity Monitoring
and Enforcement
Rights Management
Logical Controls
Application Security
Share
CMP (DLP)
Encryption
Logical Controls
Application Security
Archive
Encryption
Asset Management
Destroy
Crypto-Shredding
Secure Deletion
Content Discovery
Securosis.com

When and How to Encrypt

Laptops	Always	Full Drive or Equivalent
Desktops	Highly Sensitive	File/Folder
Portable Media	Sensitive or Always	Media or Folder
Servers	Risk Based	Varies

Securosis.com

What We've Learned

- Today, disclosures are teach us the wrong lessons
- Blame the credit card companies, not the retailers, for credit card fraud
- Consumers suffer from identity fraud, retailers from credit card fraud
- We need complete breach disclosure
- We need fraud disclosure
- We need -public- root cause analysis disclosure

Recommendations

- Encrypt your freaking laptops!
- Media gets moved, and it lasts a really, really long time, so encrypt that too!
- Encryption works well when we don't need or want access to data
- Reduce use and storage of sensitive data

Adrian Lane

Securosis, L.L.C.

alane@securosis.com
http://securosis.com
AIM: whoisadrianlane
Skype: whoisadrianlane