

# Guarding Against Data Loss



The escalation of a serious threat

Simon Hunt  
Vice President and CTO, Data Protection

September 23, 2009



## Data Breach - The escalation of a serious threat



### FINANCIAL TIMES

"DuPont scientist downloaded 22,000 sensitive documents as he got ready to take a job with a competitor..."



"TJX's \$1 billion data breach"



### Herald Tribune

The FSA has fined Nationwide £980,000 for a stolen laptop

### THE WALL STREET JOURNAL

"ChoicePoint to pay \$15 million over data breach—Data broker sold information on 163,000"

In January 2008, a USB memory stick containing classified NATO information was found in a library in Stockholm.








## Content ?

- Information on NATO's peace keeping force in Afghanistan
- Intelligence report on the attempted assassination of Lebanon's defense minister
- Intelligence report on the murder of Sri-Lanka's foreign minister

# Information - The new age currency








## Data Breach 2.0 The price of a credit card

- \$2-\$10**  
Credit card number  

- \$50-\$100**  
Birth certificate  

- \$5**  
PayPal account logon & password  

- \$30**  
Driver's license  

- \$100**  
Social Security card  

- \$200-\$300 with PIN**  
Credit card number  

- \$500-\$1,000**  
Trojan to steal account information  


# Data Breach - The escalation of a serious threat



## In 2008

- 400 Million 
- 300 Million 
- 380 Million 
- 300-400 Million 
- 2.1 Billion 

... devices used by enterprises



Over 250 privacy laws mandate Data Protection

Data Loss  
A serious business threat

- THE WALL STREET JOURNAL**  
"TJX's \$1 billion data breach" 
- FINANCIAL TIMES**  
"DuPont's email downloaded 22,000 sensitive documents as the..." 
- THE WALL STREET JOURNAL**  
"ChoicePoint to pay \$15 million over data breach..." 
- MarketWatch**  
"The FSA has fined..." 
- STRAIN**  
"Mark & Spencer was sued for over..." 

## Increasing Regulatory Pressure

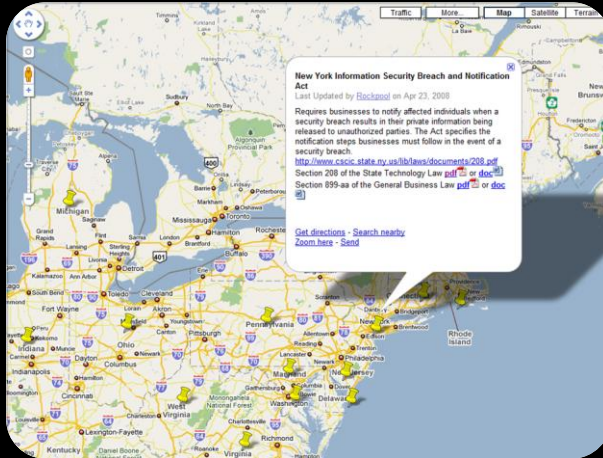
McAfee



Source: Google Maps International Crypto Law.

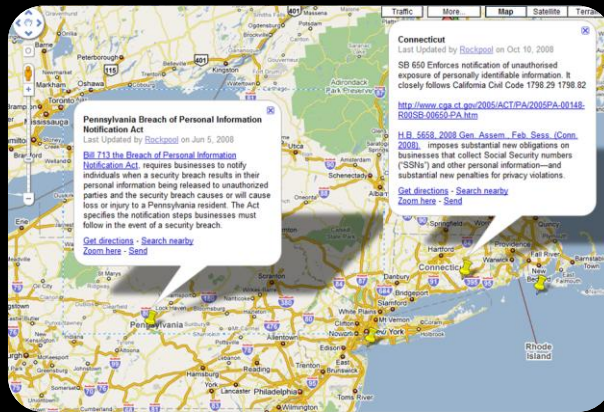
## Nevada In Detail

McAfee



Source: Google Maps International Crypto Law.

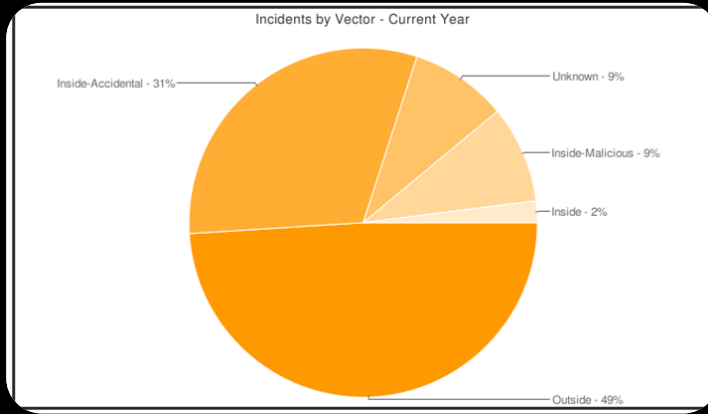
- **New York 899-aa (General Business Law)**
- "Breach of the security of the system" shall mean unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business. Good faith acquisition of personal information by an employee or agent of the business for the purposes of the business is not a breach of the security of the system, provided that the private information is not used or subject to unauthorized disclosure.
- In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such business may consider the following factors, among others:
  - (1) indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or
  - (2) indications that the information has been downloaded or copied; or
  - (3) indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.
- (a) whenever the attorney general shall believe ... that there is a violation ... bring an ...to enjoin and restrain the continuation of such violation. In such action, preliminary relief may be .. may award damages for actual costs or losses incurred by a person... impose a civil penalty of the greater of five thousand dollars or up to ten dollars per instance of failed notification, ... (b) the remedies provided by this section shall be in addition to any other lawful remedy available.



Source: Google Maps International Crypto Law.

## Incidents by Vector for 2009

McAfee

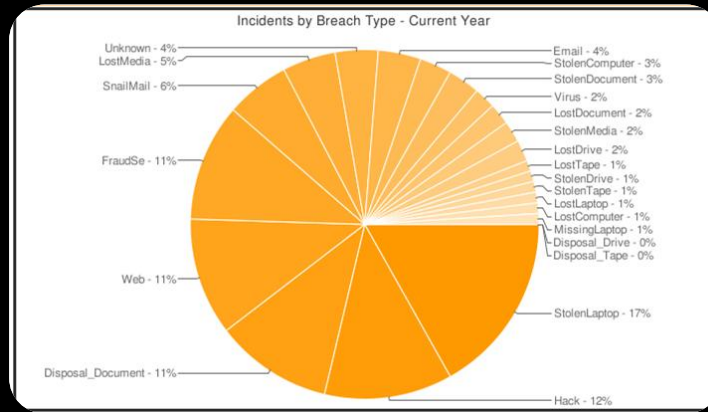


Source: DataLossDB.org

9

## Incidents by Breach Type for 2009

McAfee



Source: DataLossDB.org

10



## Data Breach - The escalation of a serious threat

McAfee

**Over 80% of the Global 5000 have no data security in place**

The perfect storm has arrived – but – most companies are still not prepared

**Data Security is incident driven ...**

**Insider steal information ?**

**Data Security is complex !**

*"Where do I begin ?"*

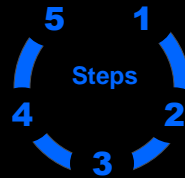
## Data Breach - The escalation of a serious threat

McAfee

Let's de-mystify the complexity of Data Protection!

Securing your information can be done ...

... in a matter of weeks – not years or months



2-10 weeks to value

13



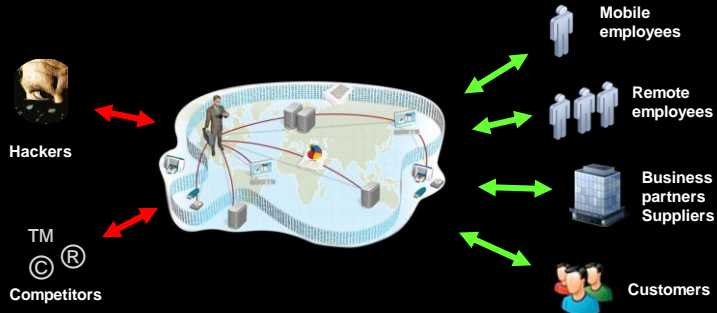
# The path to protecting your vital information

McAfee

1

Understand the Risk

Data is not static, so security cannot be static



Security MUST be "data centric"

15

# The path to protecting your vital information

McAfee

1

Understand the Risk

Data / Information is anywhere !

Data at REST

Data in MOTION

Data in USE

Desktops  
Notebooks

eMail  
Webmail

USB Sticks  
CD / DVD

0 % Secure

File Shares  
Docu Mgmt Sys

Blogs  
File Sharing

Ext. Hard drives  
Printouts



16

## The path to protecting your vital information

McAfee

1

Understand  
the Risk

### To Summarize: The First Step!

#### Data Protection needs to be tightly woven into the business

- ⇒ Sensitive and confidential information can be lost anywhere
- ⇒ The threat comes from the inside AND the outside

#### Technology is NOT the hard part

- ⇒ Aligning the business stakeholder is key
- ⇒ Raise the awareness level for the threat

#### Data protection is not a static decision

- ⇒ Information is constantly changing & travelling
- ⇒ Partners are changing, so solutions need to evolve

17

## The path to protecting your vital information

McAfee

1

Understand  
the Risk

2

Fix  
Data Encryption

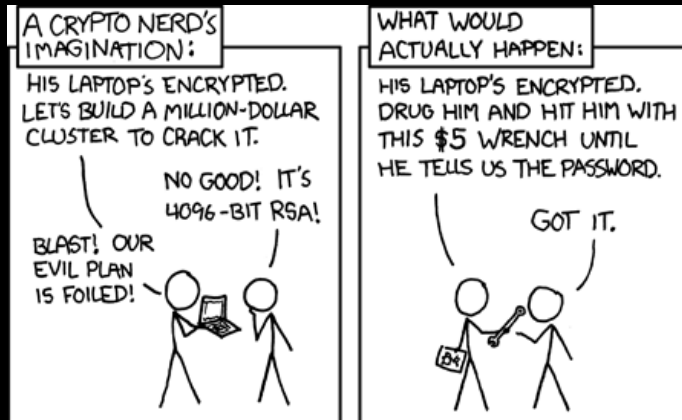
### Challenge !

- ⇒ Laptop is lost / stolen! What information was on it?
- ⇒ Non encrypted data is always considered "stolen" or "exposed"
- ⇒ Data privacy laws / regulatory compliance / corp. governance

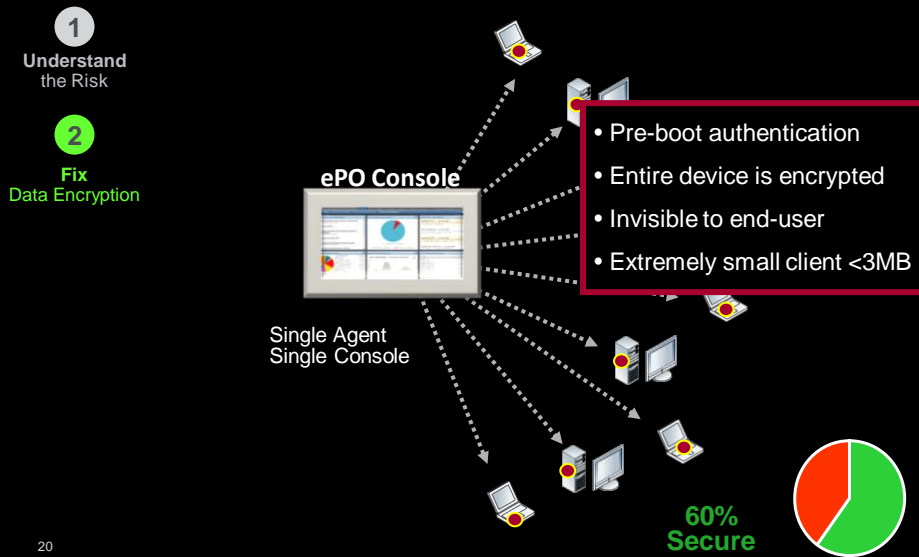
### How to fix the problem ?

1. Deploy hard drive encryption on all laptops & desktops
2. Monitor your inventory / run audit reports

18



The path to protecting your vital information



## The path to protecting your vital information

McAfee

1

Understand  
the Risk

2

Fix  
Data Encryption

### Challenge !

- ⇒ Laptop is lost / stolen! What information was on it?
- ⇒ If data was encrypted then it is not considered compromised
- ⇒ Data privacy laws / regulatory compliance / corp. governance

### How to fix the problem ?

1. Deploy hard drive encryption on all laptops & PCs
2. Monitor your inventory / run audit reports

### Time ?

- ⇒ Planning / design / policy: 1-3 weeks
- ⇒ Deployment: 2-4 weeks

60%  
Secure



21

## The path to protecting your vital information

McAfee

1

Understand  
the Risk

2

Fix  
Data Encryption

3

Manage  
Removable Media

### Challenge !

- ⇒ Information is transferred IN and OUT
- ⇒ Can be bought anywhere for \$20

### How to fix the problem ?

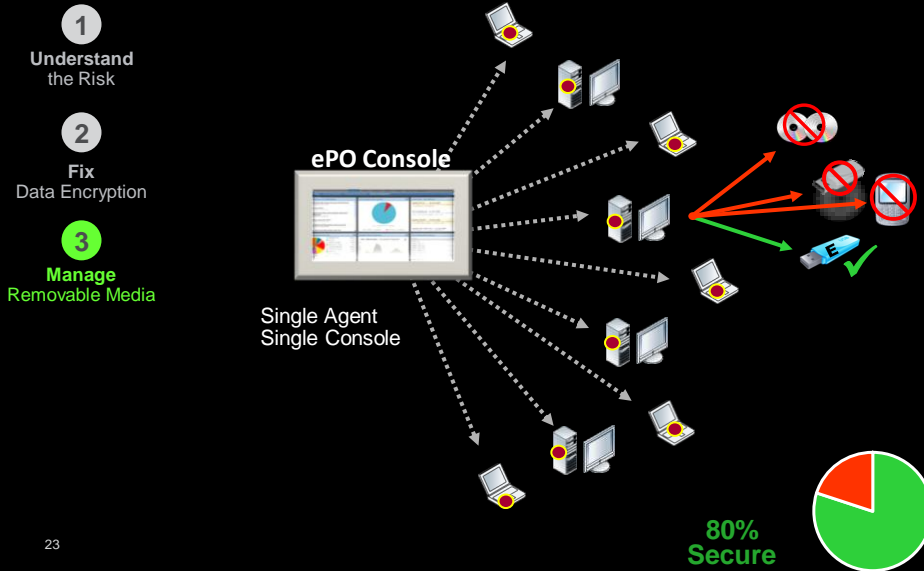
1. Encrypted USB sticks
2. Install PORT CONTROL software
3. Set policy to use only encrypted USB sticks - or set policy to encrypt data when transferred



22

# The path to protecting your vital information

McAfee



# The path to protecting your vital information

McAfee

1 Understand the Risk

2 Fix Data Encryption

3 Manage Removable Media

**Challenge !**

- ⇒ Data is transferred IN and OUT
- ⇒ Can be bought anywhere for \$20

**How to fix the problem ?**

1. Use encrypted USB sticks
2. Install DEVICE CONTROL software
3. Set policy to use only encrypt USB sticks - or - set policy to encrypt data when transferred

**Time ?**

⇒ Encrypted USB sticks:	Time to write a purchase order
⇒ Device Control Software:	1-3 weeks
⇒ Set policy for encryption:	1 week

80% Secure

24

# The path to protecting your vital information

McAfee

1

Understand  
the Risk

2

Fix  
Data Encryption

3

Manage  
Removable Media

4

Identify  
Confidential Data

## Executive directive ...

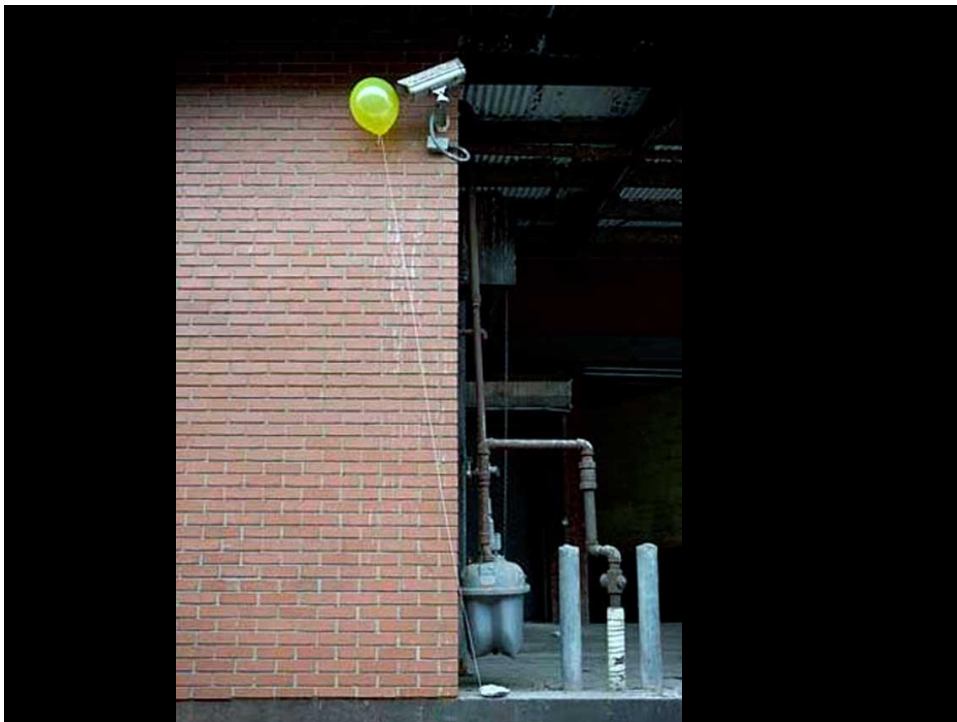
*"Make sure no confidential data  
leaks from our company! ...and  
don't interfere with the business!"*



## Simple to say, but ...

- ⇒ Data is everywhere ...
- ⇒ The office is anywhere ...
- ⇒ The people travel everywhere ...

25



# The path to protecting your vital information

McAfee

1

Understand  
the Risk

2

Fix  
Data Encryption

3

Manage  
Removable Media

4

Identify  
Confidential Data

## 1. Focus on risk drivers specific to your organization

- ⇒ Compliance, Intellectual Property (IP)
- ⇒ Business or legal information, staff related information
- ⇒ *Pick your top 1-5 most important risk drivers*

## 2. Define most critical vectors

- ⇒ Data at Rest, Data in Motion, Data in Use
- ⇒ Focus on data that travels

## 3. Determine the functional stakeholders' needs

- ⇒ Interview stakeholders; i.e. legal, HR, compliance, ...
- ⇒ Define their needs & requirements

Guide to a new generation of DLP technologies



27

# The path to protecting your vital information

McAfee

1

Understand  
the Risk

2

Fix  
Data Encryption

3

Manage  
Removable Media

4

Identify  
Confidential Data

5

Deploy  
Data Loss  
Prevention

## Three criteria for a successful DLP deployment

Know what information to protect

Ability to identify *Data Leakage*

Time for deployment

# The path to protecting your vital information

McAfee

1

Understand the Risk

2

Fix Data Encryption

3

Manage Removable Media

4

Identify Confidential Data

5

Deploy Data Loss Prevention

## DLP Essentials

Discover

Monitor

Prevent

# The path to protecting your vital information

McAfee

1

Understand the Risk

2

Fix Data Encryption

3

Manage Removable Media

4

Identify Confidential Data

5

Deploy Data Loss Prevention

## DLP Essentials

Discover

Monitor

Prevent

- Find data
- Index data
- Who has access?
- **Endpoint & network !**

Create DLP Index



similar to Google indexing

# The path to protecting your vital information

McAfee

## DLP Essentials

- 1 Understand the Risk
- 2 Fix Data Encryption
- 3 Manage Removable Media
- 4 Identify Confidential Data
- 5 Deploy Data Loss Prevention

Discover

Monitor

Prevent

- Find data
- Index data
- Who has access?
- Endpoint & network !

Create DLP Index



- Monitor data flow
- Monitor data use
- Endpoint & network !

# The path to protecting your vital information

McAfee

## DLP Essentials

- 1 Understand the Risk
- 2 Fix Data Encryption
- 3 Manage Removable Media
- 4 Identify Confidential Data
- 5 Deploy Data Loss Prevention

Discover

Monitor

Prevent

- Find data
- Index data
- Who has access?
- Endpoint & network !

Create DLP Index



- Monitor data flow
- Monitor data use
- Endpoint & network !

- Set policies
- Prevent data leakage
- Establish forensic trace
- Endpoint & network !

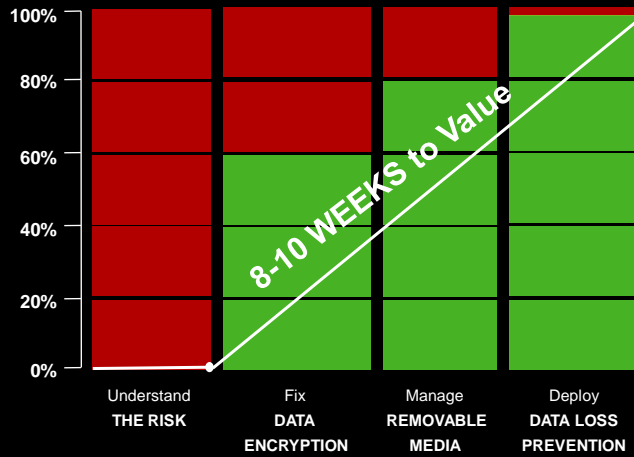
DLP in network and offline



# The path to protecting your vital information



## Data Security



33

# Independently confirmed as the Leader in DP



## 2009 Gartner Magic Quadrant



34

## 2008 Forrester Wave for DLP

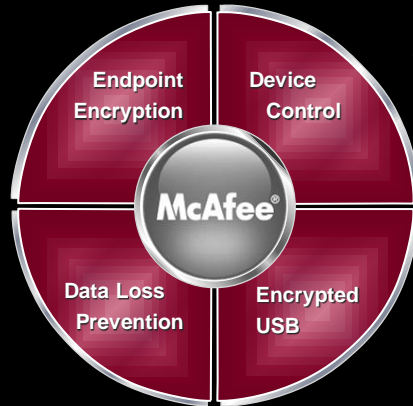


## McAfee - Guarding Against Data Loss

McAfee

McAfee's  
**\$0.7 Billion**  
investment

Over  
**6000** customers  
on over **10mill** PC's



Standard in over  
**40** Governments

In over  
**70** countries

35



**McAfee®**