Preventing data breaches…….
The role of the security industry

Ilias Chantzos, Director, Government Relations, EMEA & APJ

EDPS/ENISA workshop, European Parliament 23-10-2009

symantec.

Agenda

The current security landscape

The “anatomy” of a data breach

Our role and experiences in preventing a breach

Did You Know…

285 Million records were stolen in 2008[1]

$225 is the average cost per record breached due to malicious acts[2]

67% of data breaches happen because of the mistakes of well-meaning insiders[3]

1. Verizon Business Risk Team, ***2009 Data Breach Investigations Report***
2. Ponemon Institute, ***Cost of a Data Breach Study, 2008***
3. Verizon Business Risk Team, ***2009 Data Breach Investigations Report***

The “anatomy” of a breach

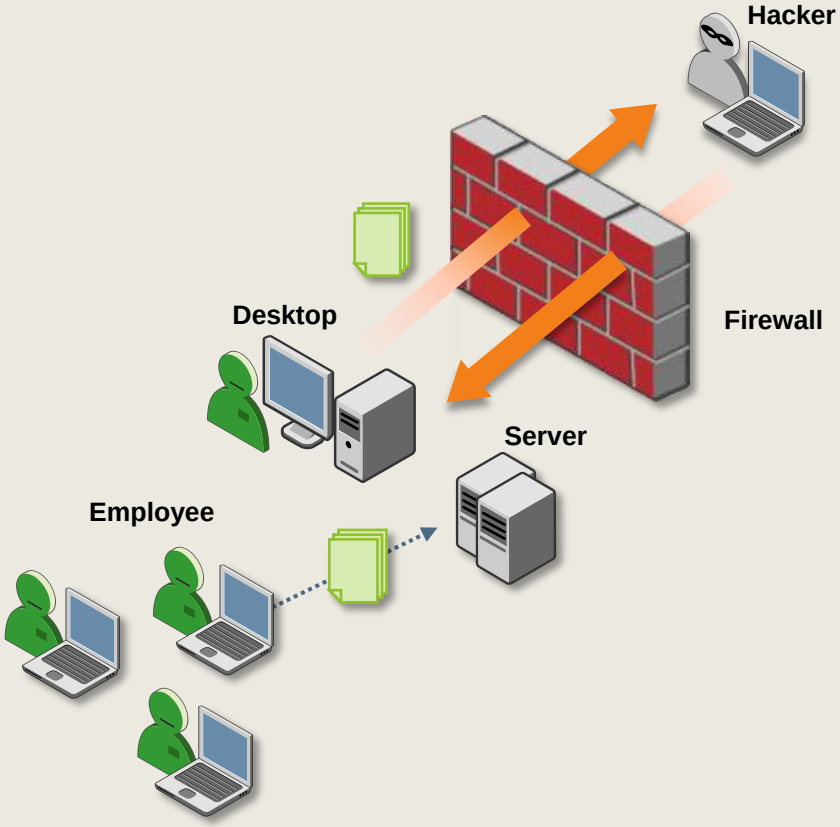
Sources Of A Breach

Well Meaning Insider

Hackers-Targeted Attacks

Malicious Insider

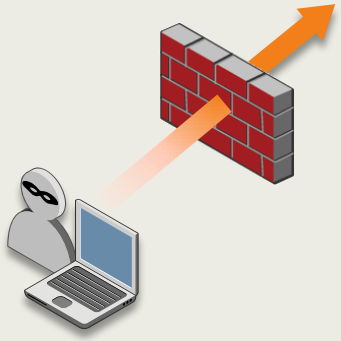
Well-Meaning Insider



"Well-Meaning Insider" Breach Sources
1. Data on servers & desktops
2. Lost/stolen laptops, mobile devices
3. Email, Web mail, removable devices
4. Third-party data loss incidents
5. Business processes

Targeted Attacks

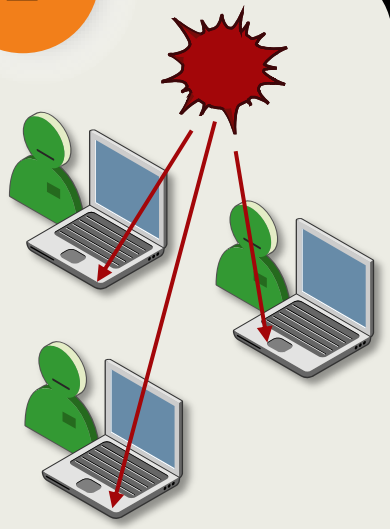
1



INCURSION

Attacker breaks in via targeted malware, improper credentials or SQL injection

2

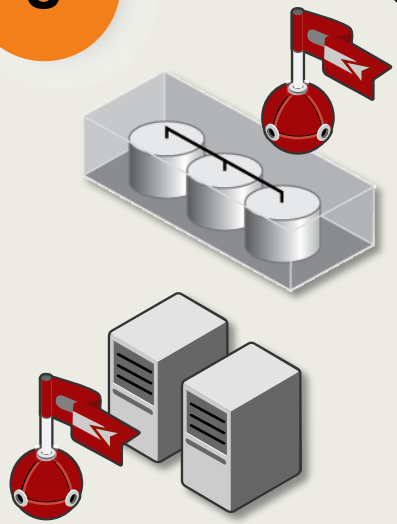


DISCOVERY

Map organization's systems

Automatically find confidential data

3

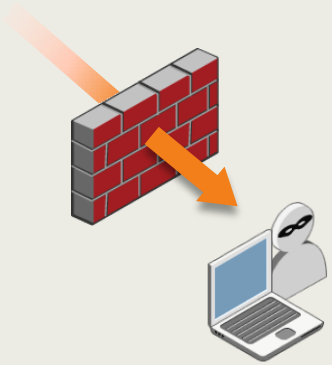


CAPTURE

Access data on unprotected systems

Install root kits to capture network data

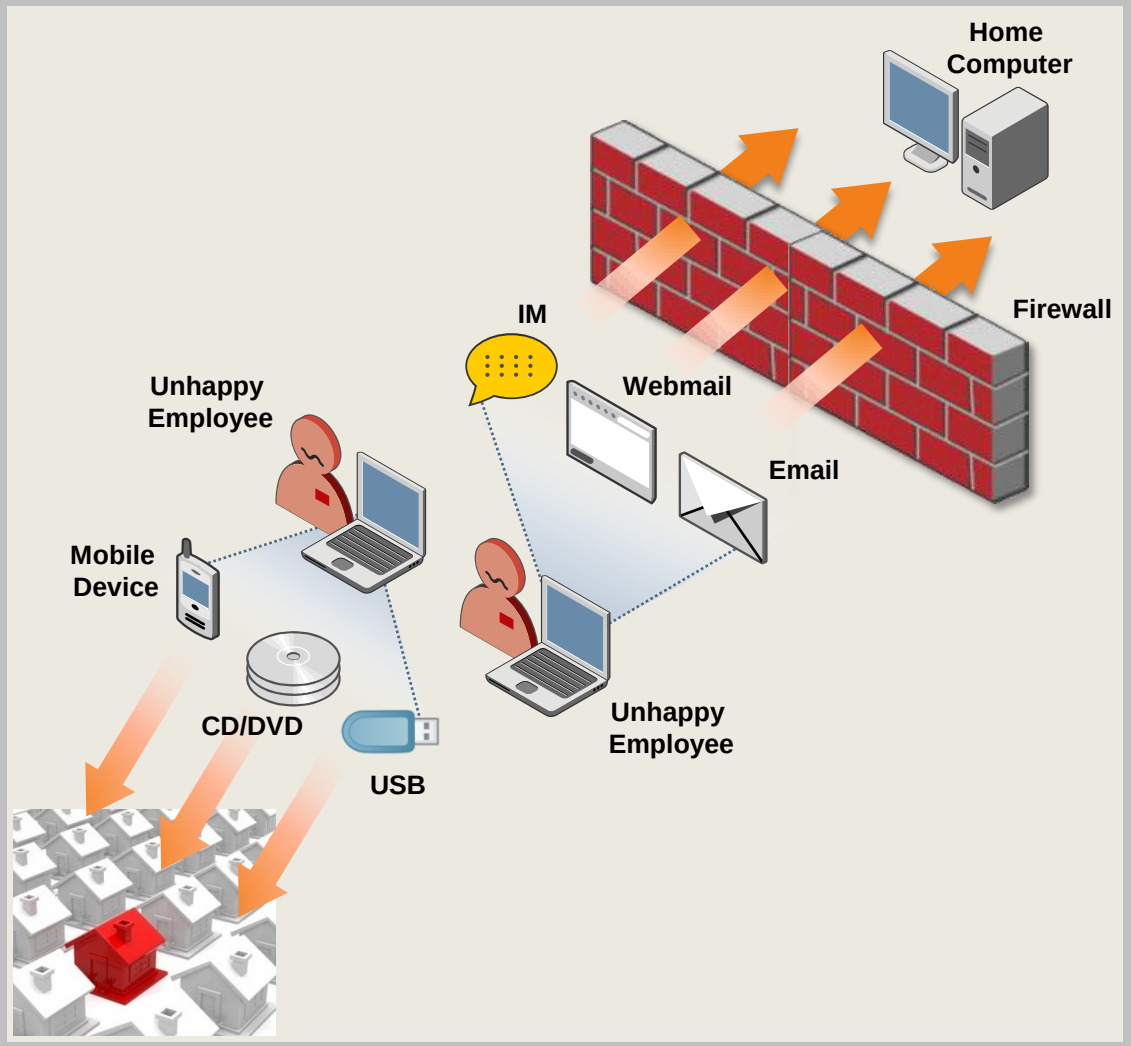
4



EXFILTRATION

Confidential data sent to hacker team in the clear, wrapped in encrypted packets or in zipped files with passwords

Malicious Insiders



Malicious Insider: Four Types

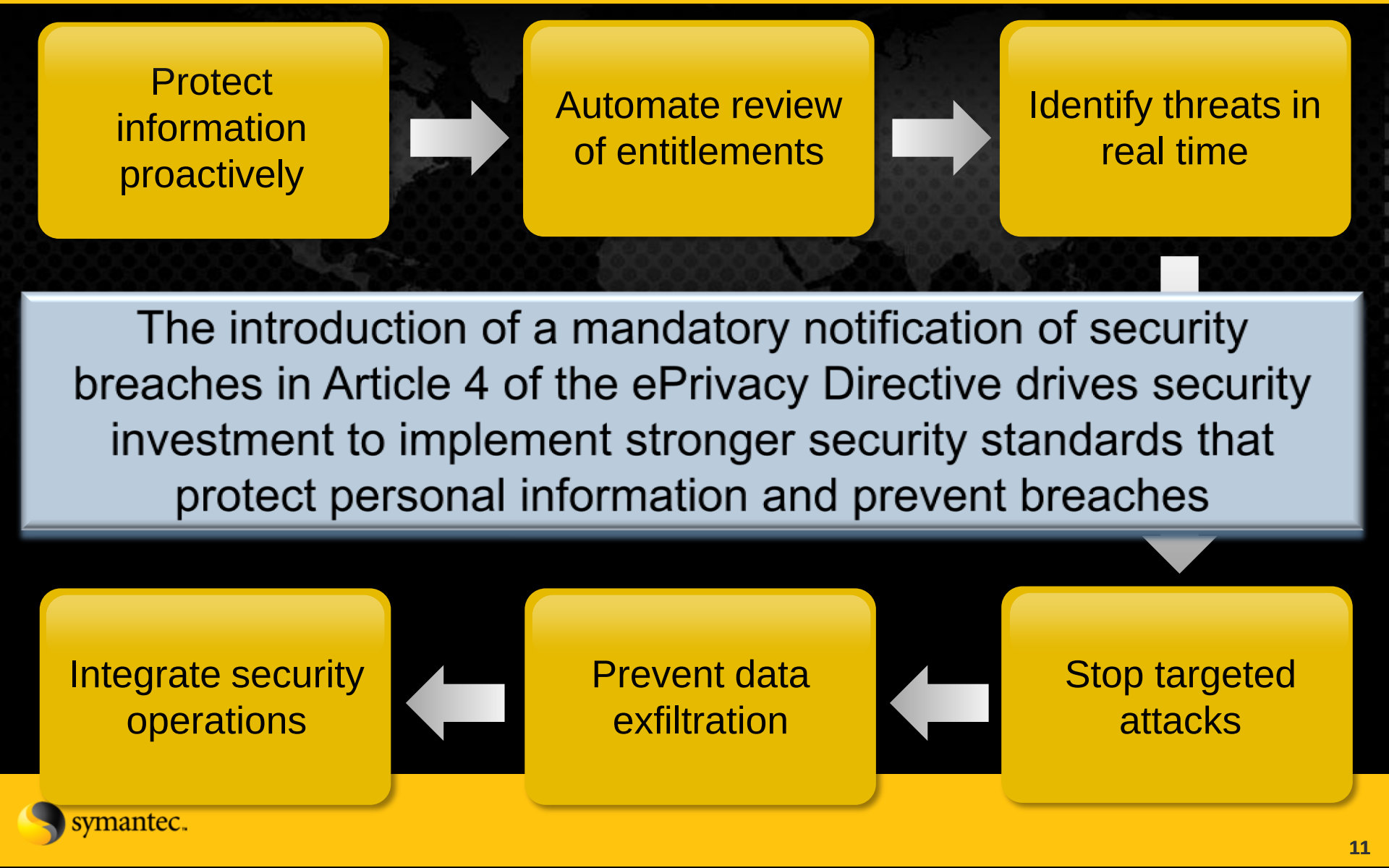
1. White collar criminals
2. Terminated employees
3. Career builders
4. Industrial spies

Our role and experience in preventing a breach

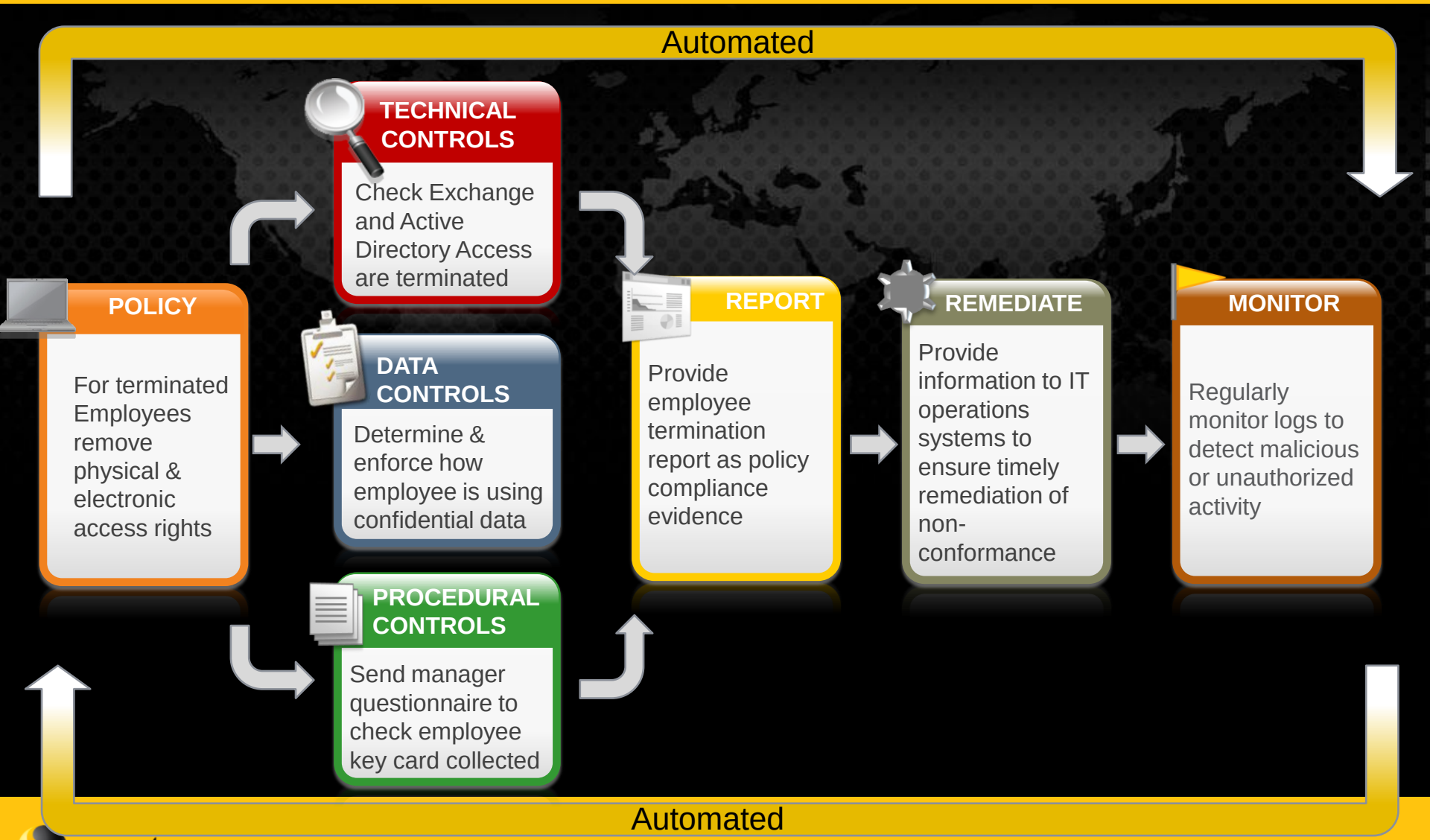
What is the role of Symantec?

- Symantec is a technology company
  - We will build innovative solutions and offer new services to address these risks
- Symantec is a trusted advisor
  - It will advise its customers and the public at large on how to address the threat
- Symantec is a corporate citizen
  - It will provide its expertise to governments to help them define policy and regulation to address the challenge in a pragmatic manner

How to Stop Data Breaches



How does it work in practice?



How Symantec has helped?

Well-Meaning Insider

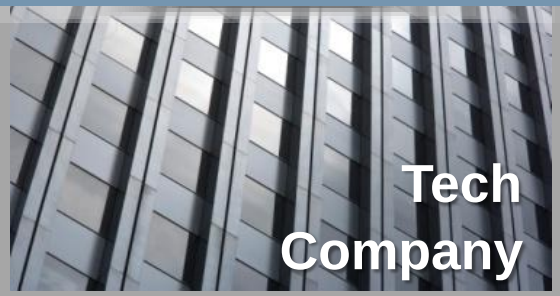
Situation

- Employee data leaving via the network
- Needed to determine scale of breach

Results

- Data on servers for application testing
- Cleaned up exposed data
- Fixed broken business process

Targeted Attack



Situation

- Network overtaken by hackers
- "Carder" ring on corporate machines

Results

- Investigations team flown out
- Aided by local law enforcement
- Prosecuted perpetrators

Malicious Insider

Situation

- Planning a reduction in force
- Rumors circulate
- Employees tried stealing data

Results

- Blocked emails containing confidential data
- Prevented loss of thousands of customer records

Some points to reflect on…..

- Every year the amount of data we produce doubles
- Information is the currency of the new age
  - The bad stuff is more than the good stuff
- More and more people go online
  - China has more users than the US
- New technologies and services are offered
  - Cloud computing
  - Virtualisation
  - Social networks

BREACHES ARE BOUND TO HAPPEN

Thank You!

Ilias Chantzos

ilias_chantzos@symantec.com

+3225311161