



What does security mean in today's mobile environment?

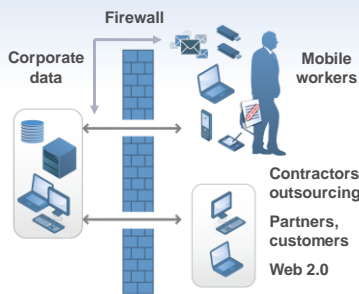
Richard Jacobs, CTO, Sophos Plc

March 2009

SOPHOS

Changing security landscape

Digital generation set loose



Information theft – not graffiti

Complex threats....



Fast changing



Targeted



Web-based, Invisible

...targeting commercial data



Personally identifiable information



Intellectual property



Customer data

Regulatory disclosure and reputation damage



CSB 1386

PCI-DSS

GLBA



95/46/EC

HIPAA

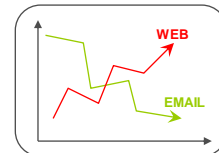


Threat evolution

- Viruses, worms, spam, spyware & rootkits
- Overflows and exploits
- Information leakage & control
- Regulation

Some brief statistics

- 20,000 previously unseen files received each day
 - 85% proactively detected
- Malicious URLs discovered every **5 seconds**
- ~97% of business email is spam
 - But volume of email that carries malware – 1:416
Trend had been down until recently
- Web is now the main attack vector
 - 83% of malware comes from hijacked sites
 - Automation, server-side scripting



High volume, professional, conveyor belt of financially motivated malware...

Accelerating threat

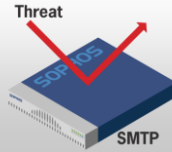
- Network spreading using exploits
 - Blaster – 72 days after disclosure (2003)
 - Sasser – 18 days after disclosure (2004)
 - Vanebot – 12 days after disclosure (2006)
- MS08-67 on 23 October 2008
 - Serious remote execution vulnerability in Windows
 - Troj/Gimmiv-A – in the wild before disclosure (reason for out of band update) – not self replicating
 - Conficker...

Conficker

- Millions of infected PCs, despite patch availability
- Multiple infection vectors
 - Vulnerability
 - USB device
 - Weak passwords
- Polymorphic control lookup
- Coordinated international response

Threat delivery using compromised web sites

Email defended



Easy targets for infection



Easy to find you

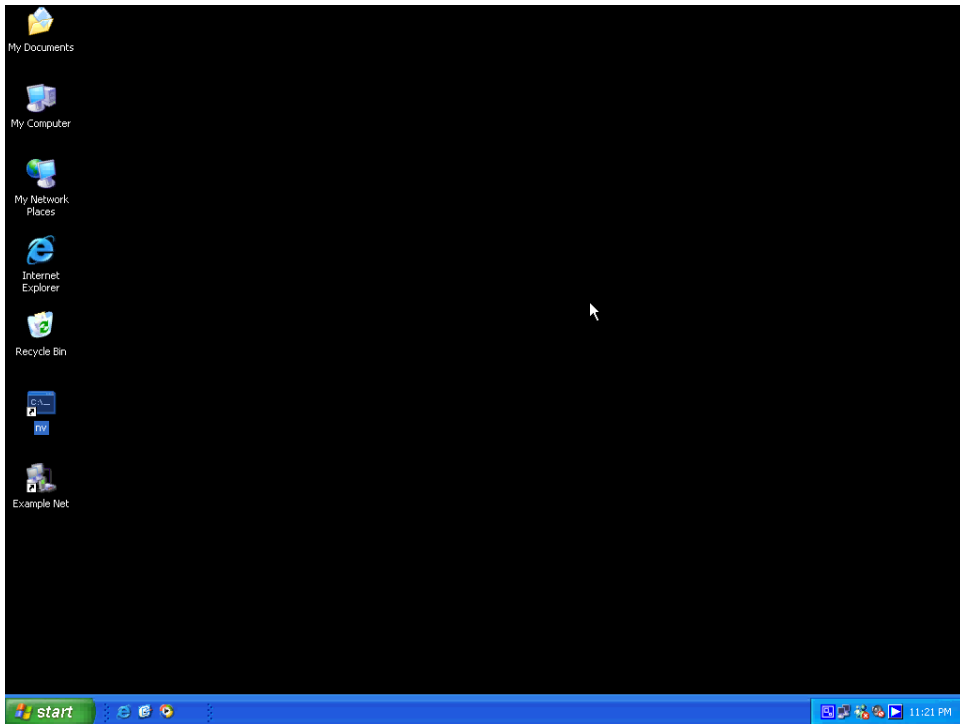
83% of threats come from hijacked sites

Source: Sophos Security Threat Report, January '08



SophosLabs™ identifies a newly infected web page every 5 seconds.

FakeAlert distribution sites – “professional”



Smartphone malware

- Symbian
- Microsoft
- Blackberry
- iPhone

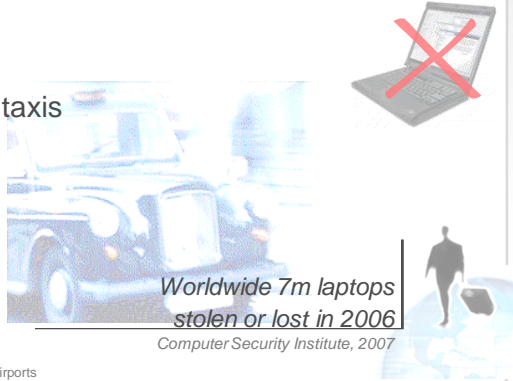
- Lack of homogeneity
- Increasing use of full OSes
- Malware is a social attack

Rise of stolen/lost Confidential Information

- 3.300 Laptops lost or stolen weekly at the eight largest airports in EMEA
- 12.000 laptops lost or stolen weekly in US airports (estimated)



July 2008
www.vnunet.com/vnunet/news/2223012/eu-travellers-losing-laptops-airports

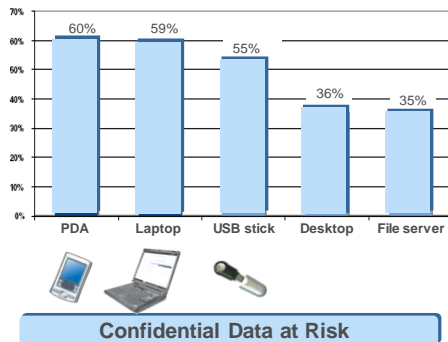


Worldwide 7m laptops
stolen or lost in 2006
Computer Security Institute, 2007

- **5000** laptops left in London taxis during a 6 months period

www.theregister.co.uk/2005/01/25/taxi_survey

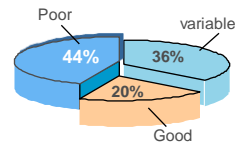
What is the probability that devices contain unprotected confidential data?



Ponemon Institute
U.S. Survey: Confidential Data at Risk, August 2007

How would you rate your employees' attitude towards mobile security?

Freedom Dynamics, Feb. 2007, Secure Mobile Working



70% of all company data is stored redundant on Endpoints (notebooks, desktops, USB Memory sticks), not only on servers

Ponemon Institute: Confidential Data at Risk, 2006

What is mobility?

Your workers

- Home
- Hotels, airports, customers
- Internet cafés
- Your offices
- Anywhere, anytime on any device

Your visitors

- Guests
- Contractors
- Partners
- Employees?



13

Mobility accelerators

- Consumer technology
 - Faster, cheaper, easier
 - Web 2.0
 - iPhone, Android...
 - Netbook
- Economy
- Software as a Service
 - Google Docs, Salesforce, Azure...
- Desktop virtualization

14

Challenge of embracing digital generation

Business challenges

- Enable mobility and web 2.0
- Comply with regulation
- Avoid business disruption
- Avoid damaging information disclosure



Operational challenges

- Enable business process innovation
- Minimize impact on users
- Minimize operational costs
- Manageability
- **You're not in control**



Mobile security priorities

Prioritise what you're protecting

- Users
- Devices
- Data
 - Personal or intellectual property?
- Productivity
- Reputation
- Customers
 - Users, devices...

17

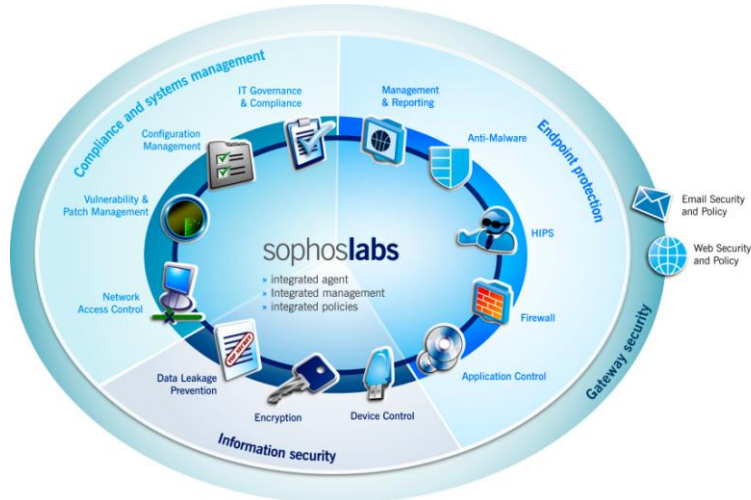
And what you're protecting against

- Internal
 - Accidents
 - Attacks
- External

- Data
 - Disclosure, prosecution, or compliance?
 - Be honest!

18

Comprehensive security and control



Mobile security technologies

- Configuration management
 - Passwords & PINs
 - Port control
- Encryption
 - Fixed and removable media
- Remote wipe
- Anti-malware
- Network Access Control

Building security policies

- Don't run before you can walk
- Don't use product configuration as a proxy for policy definition
- Ensure consistency between PCs and other devices
- Assume that every device is connected directly to the Internet
- Include users
 - You can't control them
 - You can alienate them

21

Simplicity and manageability

Simplicity
delivers

Better security

- Reduces opportunity for mis-configuration 
- Comprehensive capabilities, without agent pollution 
- Industry leading threat protection, ensures compliance 

Least investment

- Reduces operational complexity 
- Minimises training & need for deep security expertise 
- Quality and responsive support/service 



What does security mean in today's mobile environment?

Richard Jacobs, CTO, Sophos Plc

March 2009