Practical SME Security on a Shoestring

By Matt Summers

Agenda

- **Who am I?**
- **What is security?**
- **Why all SMEs need to care**
  …. but without fear
- **The Hype Curve**
- **How incidents happen**
- **Security on a shoestring**

Matt Summers

- Penetration tester and security researcher
- Doing something in security for 19 years
- Work for small businesses, large enterprises, vendors AND consultancies

Some background

What is security?

“Security is a degree of resistance to, or protection from a threat.”

Security provides:
"a form of protection where a separation is created between the assets and the threat."

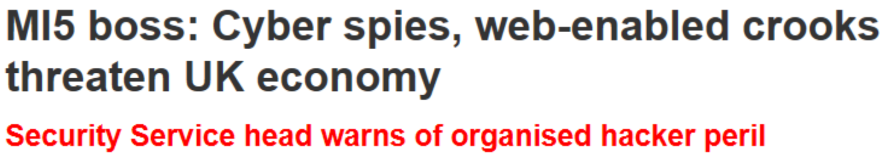
Key facets of successful security

- Processes and procedures
  - What is expected within the business
- People
  - Who are trained
  - Who have a sense of risk ownership
  - Who don’t feel afraid to report
- Technology
  - Helps people
  - Technology on its own can’t solve cyber security

The threat is real

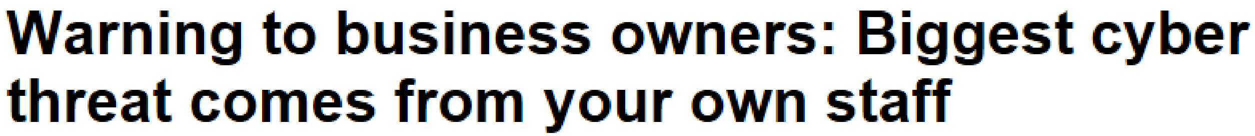
GCHQ warns private sector bosses of unprecedented cyber-attack threat

Ministers and intelligence agencies say businesses are failing to do enough to protect themselves from cyberthreats

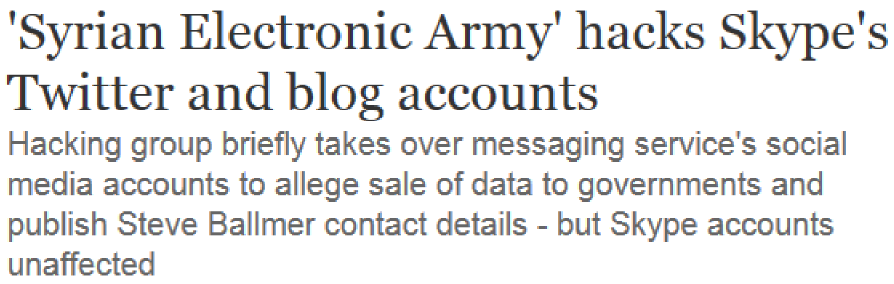


MI5 boss: Cyber spies, web-enabled crooks threaten UK economy

Security Service head warns of organised hacker peril



Warning to business owners: Biggest cyber threat comes from your own staff



'Syrian Electronic Army' hacks Skype's Twitter and blog accounts

Hacking group briefly takes over messaging service's social media accounts to allege sale of data to governments and publish Steve Ballmer contact details - but Skype accounts unaffected

Barclays hacking attack gang stole £1.3 million, police say

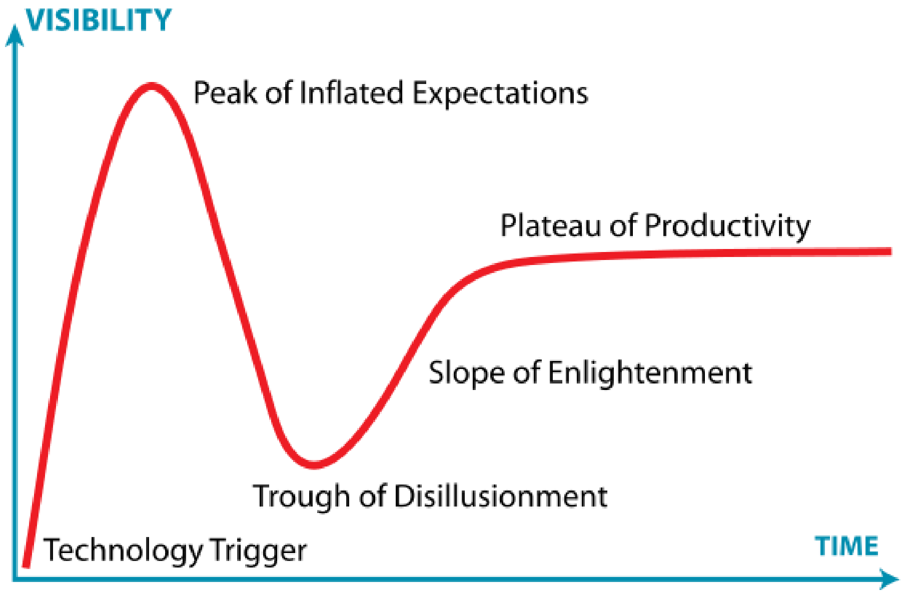
A gang of hackers stole £1.3 million by hijacking the computer system of a branch of Barclays Bank, police have claimed as they arrested eight men.

Who are Their Targets and Why?

- Casual
  - Target: Anything
- Criminals / Employees
  - Target: SME On-Line Banking
  - Target: Extortion (e.g. CryptoLocker)
- State Sponsored
  - Very targeted attack
  - Target: IP
  - Target: System (disruption)

Anti-Virus Alone is Not Enough

The "Hype Cycle"



The “Hype Cycle”

- Anti-Virus
- Firewalls
- Whole Disk Encryption
- Data Leakage Prevention
- Web Application Firewalls
- SIEM
- etc.

How incidents happen: Staff

- Don’t have the training
- Don’t know what to do if they suspect something
- Fear punitive responses to mistakes
- Thinks the technology makes risk someone else's problem

How incidents happen: No Controls

- Outdated technology
- No Anti-Virus
- Flat computer networks
- Shared passwords
- Weak passwords
- Unencrypted laptops and USB sticks

How incidents happen: Control Failures

- Outdated Anti-Virus
- Unpatched systems
- Weak WI-FI network security
- Sharing passwords to help
- Misuse of work systems
- Lost devices
- Theft

nccgroup
freedom from doubt

Security for SMEs on a Shoe String

Security on a shoestring

Is it possible to do security on a shoestring?

Yes!

How?

Controls

“Security controls are safeguards or countermeasures to avoid, counteract or minimize security risks relating to personal property, or any company property.”

Controls

Preventative

- Attempt to stop an event from occurring

Detective

- Identify and alert when the event occurs

Corrective

- Remediate after the event has occurred

Controls

Physical

- Fences, locks

Procedural

- Policies, standards and processes

Technical

- Firewalls, anti-virus, encryption

Legal and Regulatory

- Jurisdictional law, PCI-DSS

Controls

- Cyber Streetwise

  www.cyberstreetwise.com

- CPNI Top 20 Controls

  based on SANS

  www.cpni.gov.uk/advice/cyber/Critical-controls/

Top 20 Controls

Critical control 1 - Inventory of authorised and unauthorised devices

Critical control 2 - Inventory of authorised and unauthorised software

Critical control 3 - Secure configurations for hardware and software

Critical control 4 - Continuous vulnerability assessment and remediation

Critical control 5 - Malware defences

Critical control 6 - Application software security

Critical control 7 - Wireless device control

Critical control 8 - Data recovery capability

Critical control 9 - Security skills assessment and appropriate training to fill gaps

Critical control 10 - Secure configurations for network devices

Critical control 11 - Limitation and control of network ports, protocols, and services

Critical control 12 - Controlled use of administrative privileges

Critical control 13 - Boundary defence

Critical control 14 - Maintenance, monitoring, and analysis of security audit logs

Critical control 15 - Controlled access based on the need-to-know

Critical control 16 - Account monitoring and control

Critical control 17 - Data loss prevention

Critical control 18 - Incident response capability

Critical control 19 - Secure network engineering

Critical control 20 - Penetration tests and red team exercises

If you do 7 things…

- Explain that staff are the first line of defence
- Teach staff about phishing
- Use strong passphrases
- Get rid of Windows XP, Office 2000, Internet Explorer 6
- Update software (Adobe, Java, IE)
- Use up-to-date anti-virus
- Test your recovery processes

Longer term strategies..

- Perform risk assessments
- Implement a level of the 20 CSC
  - Harden devices
  - Segregate your network
  - Limit and control administrative privileges
  - Limit and control network services
  - Encrypt your USB sticks / laptops
  - Create an IR plan

Always remember

- Don’t buy product vendor hype
- Cyber security is not about products
- Cyber security doesn’t have to be costly
- An incident will happen so have a plan

Further Reading and Resources

- www.nccgroup.com
- www.cpni.gov.uk
- www.cyberstreetwise.com
- www.sans.org
- www.cissecurity.org
- www.owasp.org

Fin

Questions?

nccgroup
freedom from doubt

Europe

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Munich

Amsterdam

Zurich

North America

Atlanta

Chicago

New York

San Francisco

Seattle

Austin

Australia

Sydney