The Cyber Security Threat to SMEs

Tony Dyhouse, 19th September 2011

ICT Knowledge Transfer Network

QinetiQ
Who’s out to get me?

The many people who care about your data
1. Script Kiddies

Who?

- Bored teenagers
- Live in online social world where they build their hacking skills
- Don’t know where or how to use these skills

Why?

- Ego
- Practice skills
- Impress peers
2. Hacking groups

Who?
- Loosely connected online groups of script kiddies

Why?
- Ego
- Impress friend, outdo each other
3. (H)Activists

Who?

- Groups of hackers connected by a cause, eg Anonymous, Lulzsec
- Use hacking skills to attack organisations they dislike
- Frequently find new causes… sometimes ask!

Why?

- Disagree with something your company does – pollution, business practices, employee treatment
- Dislike of business in general (anti-capitalist)
- Targets may not be rational, or have a clear motive
- Want to cause damage and disruption
4. Serious hackers

Who?
- Highly skilled hackers
- Often employed by organised criminals or nation states

Why?
- Steal sensitive data for profit
- Leave no trace
- Ultimate failure to damage system or be discovered
5. Organised crime

Who?

• Highly organised and skilled groups
• Have vast botnets at their control which monitor for sensitive information and infect other computers
• Use data to steel identities
• Sell data to fraudsters and blackmailers

Why?

• Make vast amounts money
6. Nation states

Who?

• Arms of national governments
• Steel huge amounts of data and filter for something useful

Why?

• Steel data of value to their country
• Intellectual property, research, corporate deals, military plans
What can you do about it?

*Simple precautions to minimise the risk of compromise*
1. Good Practice

Risk Management

– Define (critical) Assets
– Define Threats and vulnerabilities
– Assess Impact
– Document
– Spend Budget
– Measure!
2. Good Practice

People.

Process.

Technology.

Your staff are your weakest link.

- Ensure staff have basic security training, eg, what constitutes a suspicious email
- Develop basic security policies, eg, password protect phones and laptops - AUP
- Staff of 3rd party providers become yours
- Background checks

When you’re up to your neck in alligators, it’s easy to forget that the initial objective was to drain the swamp.

– Starter and leaver process
– Near miss incident reporting
– REGULAR awareness briefings with examples
– Code of Connection for 3rd parties
– If you don’t need it don’t keep it. Thinning process
– Backup. Restore!
– Secure disposal
– Incident response and recovery (DR, BCP)
5. Good Practice. Technology.

Don’t bin the firewall yet!

– Layered defences - AV
– If you don’t need it disable it
– Not just for compliance – Information (lots of it)
– Ensure required level of competence available
– Update and patch
– Pentest!
Thank You

Tony Dyhouse

tony.dyhouse@ictktn.org.uk