skillcast®

Cyber Security Training Presentation

[name] [date]

Learning objectives

- Understand the scale of the threat
- Know who our adversaries are and what they can do
- The red flags to look for
- Our company's cyber security policy

skillcast®

What is a security incident?

Security incidents are:

"... attempts to gain unauthorised access to a system or data

… modification of firmware, software or hardware without consent

… unauthorised use of systems or data

…malicious disruption or denial of service…"

And significant incidents:

"…impact on the UK's national security or economic wellbeing

…impact on the continued operation of an organisation"

National Cyber Security Centre

The scale of the threat

We fight 50,000 cyber attacks a day
CEO, energy company, EY report

UK businesses faced a 22% increase in cyber incidents over the last year
IT Pro

2 million computer misuse offences every year
BBC website

UK businesses lost to cyber crime were
£1 billion+
IT Pro

Cyber incidents are on the rise…

Who commits cybercrime?

Nation States

YES

Script Kiddies – teens doing it for the kudos

YES

Organised criminal gangs

YES

Hacktivists

YES

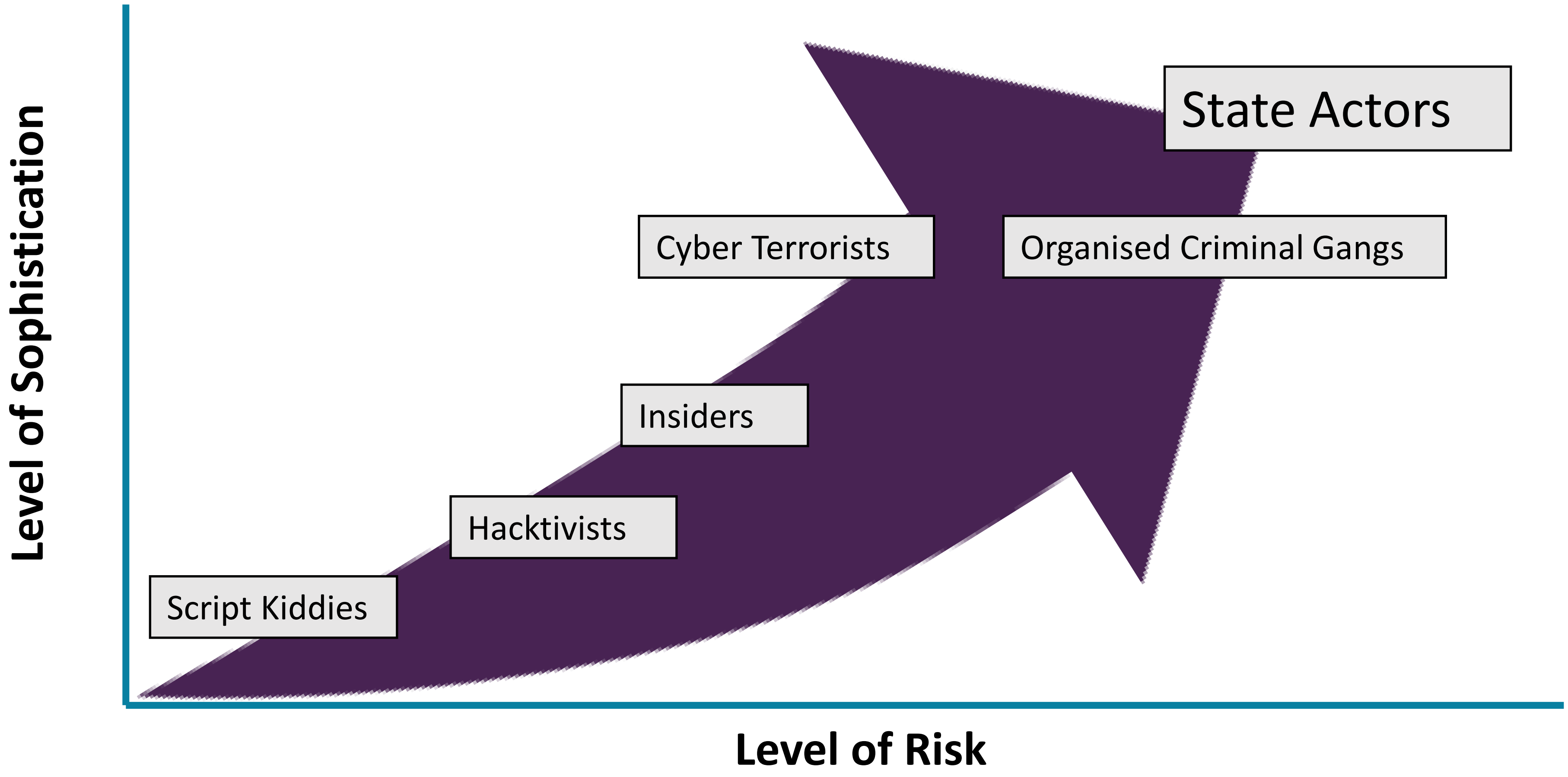
Cyber terrorists

YES

Insiders

YES

Who are our adversaries?



What are the motivations?

1. Financial gain
2. Espionage/Intelligence

What cyber criminals do: techniques

Hacktivists	Buying compromised data, low-end malware, basic DDoS, exploiting known vulnerabilities
Cyber terrorists	Basic DDoS, buying in services
Organised criminal gangs	Malware development, targeted emails, other attack tools bought on market
Nation states	Watering hole, advanced DDoS, targeted emails, zero-day exploits
Insiders	Data theft, sharing logins and escalating privileges

When it goes wrong

Boy, 17, admits TalkTalk hack, which affected 157,000 customers

Polish banking system hacked

Cyber thieves stole £2.5m from Tesco Bank accounts

Russians accused of cyber breaches in run-up to US elections

Financial and reputational damage

Incidents can cost up to **£2.6 million** (PWC report)

Average cost of a breach **£600k-£1.15m** (NCSC)

73% of customers would reconsider using a company that lost or failed to keep their data safe (Deloitte survey)

TalkTalk

Yahoo

Sony

skillcast®

How they attack

- Phishing, smishing or vishing
- Social engineering
- Impersonation - of suppliers, senior managers, the Police
- Coercion
- Malware and Trojans
- Pharming and spoof URLs (fake sites)
- Physical access

You make the call: What type of attack is it?

“I got an email from my bank telling me to click on a link to update my PIN"

Phishing ✓

Social Engineering

Malware

Coercion

You make the call: What type of attack is it?

“The site looked so genuine – the logo was exactly the same. But my partner spotted that it was spelt ‘ebayy’ not ‘ebay’"

Phishing

Social Engineering

Malware

Pharming or spoof URL ✓

You make the call: What type of attack is it?

“I found a USB in the carpark – I was only trying to find out who it belonged to. How was I to know it contained a virus?"

Phishing

Social Engineering

Coercion

Malware ✓

You make the call: What type of attack is it?

“I was messaging a friend of a friend on Facebook. He said he used to work with me. I didn’t remember. Then, he tried getting me to pass on inside information.”

Phishing

Pharming

Coercion ✓

Malware

Our Cyber Security Policy

1. Encouraging everyone to get involved
2. Appointing people with responsibility for cyber security
3. Having an incident management plan – so we know what to do
4. Requiring everyone to read and implement our Cyber Security Policy

Do…

- ✓ **Read our Company's Cyber Security Policy** - make sure you understand the rules and why they're important
- ✓ **Be vigilant** - cyber criminals can attack anywhere, when you're working at home, travelling on the Tube, on your way to a meeting, etc
- ✓ **Keep anti-virus software up-to-date** - download updates or patches as soon as they're available
- ✓ **Promptly report signs your device may be infected** - e.g. high CPU, slower response, duplicated files, ghosting
- ✓ **Keep backup copies of all data** - this makes us less vulnerable to ransomware attacks
- ✓ **Tell your manager** - if you click on a link or download something by accident – the sooner we know, the quicker we can resolve it

Don’t…

- ✗ Respond to or click on the links in unsolicited emails
- ✗ Advertise where you work on social media profiles - keep information to a minimum (you may be targeted because of where you work)
- ✗ Download unauthorised software to our IT systems
- ✗ Connect external devices to our network – e.g. USBs. If you find a USB, hand it in to IT
- ✗ Access social media, gaming or adult sites using work devices – as well as breaching our conduct rules, they are often infected with malware
- ✗ Use public WiFi to connect to our data or network – anything you type can be seen by others!

Questions, comments or concerns?

Next steps

Call _____ on _____ if you need information or guidance

Call _____ on _____ if you need to raise concerns

Access self-study courses on our e-learning portal for further training [or optionally – Complete your mandatory training on our corporate e-learning portal]

About Skillcast

- Skillcast provides digital learning content, technology and services to help you train your staff, automate your compliance processes and generate management reports to help you keep track of it all.

- Our best-selling Compliance Essentials Library provides a complete and comprehensive off-the-shelf compliance solution for UK businesses.

  Register for a free trial at https://www.skillcast.com/free-trial

Copyright © 2022 Skillcast. All Rights Reserved.