

CYBER PRESENTATION

(Advice for Business)

Chris White CISMP

Police Cyber Security Advisor



@SECyberprotect



SECyberprotect

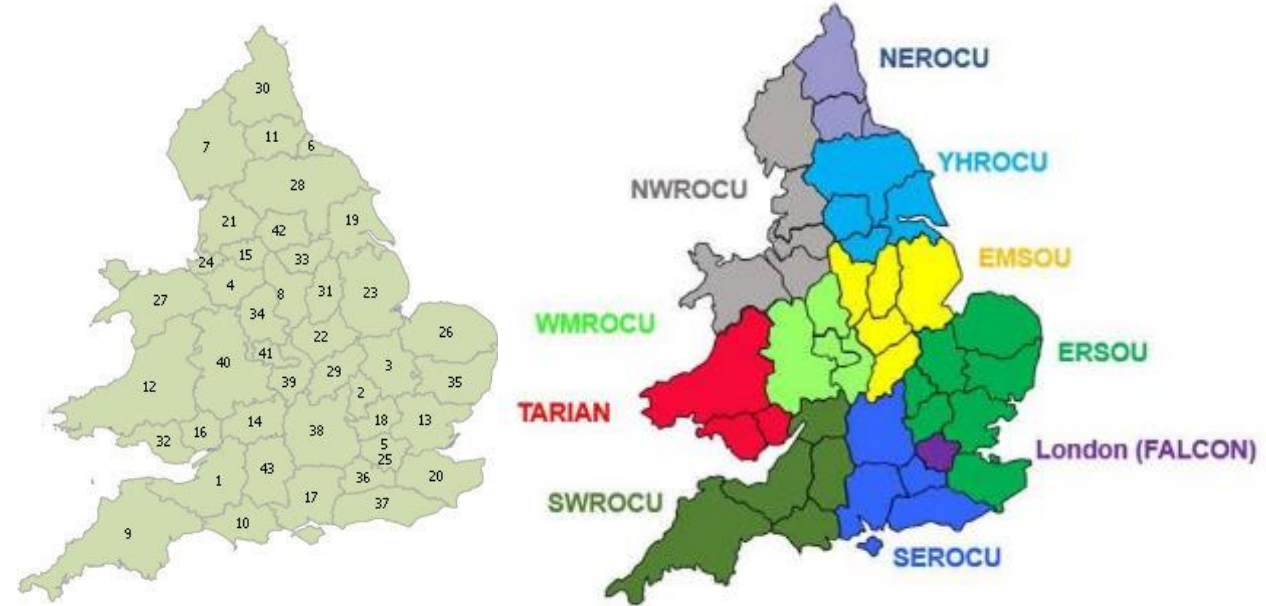
SEROCU
Cyber Protect



South East ROCU
Cyber Protect



WHO ARE WE?



Our Aims

- Gather Intelligence
- Investigation serious Cyber Crime
- Protecting / Preventing major cyber threats

Focussing on

- Cyber dependant crime - Ransomware; Data Breaches; Data Theft; Extortion; DDOS
- Cyber enabled fraud - CEO; Mandate; Fake Invoice
- Inside Threat - Data theft; Damage; Fraud



CYBERCRIME IN NUMBERS

- Av. age of UK Cyber offender is 17 yrs old compared to traditional crime offender of late 20's
- 32% of UK organisations had a Cyber attack in the last 12 months²
- Action Fraud receive 23,000 Phishing reports a month²
- 1 in every 11 recorded crimes is a Cyber Crime³
- 2018/19 saw a 1.4% increase of Cyber dependant crime¹

1 – Cyber National Assessment 2019

2 – Cyber Security Breach Survey (CSBS) 2019

3 - ONS Crime Survey for England and Wales (CSEW) 2019

This is why you should disable access to the server room before firing your IT guy.



CYBERCRIME IN NUMBERS

89% of companies rely on a technical solution

BUT 72% of breaches are via email

AND ONLY 29% of staff get cyber training²

1 – Cyber National Assessment 2019

2 – Cyber Security Breach Survey (CSBS) 2019

3 - ONS Crime Survey for England and Wales (CSEW) 2019

1

Cyber Security: Small Business Guide Actions



2

National Cyber Security Centre

a part of GCHQ

WEEKLY THREAT REPORT



3

Response & Recovery Small Business Guide



How to prepare your response to (and plan your recovery from) a cyber incident.

4

Board Toolkit



Helping board members to get to grips with cyber security



Stay Safe Online Top tips for staff

Regardless of the size or type of organisation you work for, it's important to understand why you might be vulnerable to cyber attack, and how to defend yourself. The advice summarised below is applicable to your working life and your home life. You should also familiarise yourself with any cyber security policies and practices that your organisation has already put in place.

Advisory: The rise of O365 compromise and how to mitigate

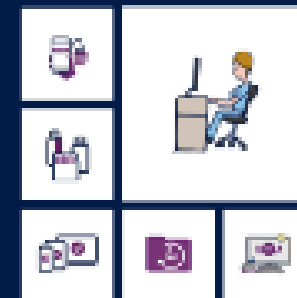
Cyber Security: Small Business Guide



How to improve your cyber security within your organisation - quickly, easily and at low cost.

Cyber Security: Small Charity Guide

How to improve cyber security within your charity - quickly, easily and at low cost.



Who is behind cyber attacks?

- Online criminals**
Are really good at identifying what can be monetised, for example stealing and selling sensitive data, or holding systems and information to ransom.
- Foreign governments**
Generally interested in accessing really sensitive or reliable information that may give them a strategic or political advantage.
- Hackers**
Individuals with varying degrees of expertise, often acting in an untargeted way - perhaps to test their own skills or cause disruption for the sake of it.
- Political activists**
Out to prove a point for political or ideological reasons, perhaps to expose or discredit your organisation's activities.
- Terrorists**
Interested in spreading propaganda and disruption activities, they generally have less technical capabilities.
- Malicious insiders**
Use their access to an organisation's data or networks to conduct malicious activity, such as stealing sensitive information to share with competitors.
- Honest mistakes**
Sometimes staff, with the best of intentions just make a mistake, for example by emailing something sensitive to the wrong email address.

Defend against phishing attacks

Phishing emails appear genuine, but are actually fake. They might try and trick you into revealing sensitive information, or contain links to a malicious website or an infected attachment.

- Phishers use publicly available information about you to make their emails appear convincing. Review your privacy settings, and think about what you post.
- Know the techniques that phishers use in emails. This can include urgency or authority cues that pressure you to act.
- Phishers often seek to exploit 'normal' business communications and processes. Make sure you know your organisation's policies and processes to make it easier to spot unusual activity.
- Phishers often seek to exploit 'normal' business communications and processes. Make sure you know your organisation's policies and processes to make it easier to spot unusual activity.
- Anybody might click on a phishing email at some point. If you do, tell someone immediately to reduce the potential harm caused.

Secure your devices

- The smartphones, tablets, laptops or desktop computers that you use can be exploited both remotely and physically, but you can protect them from many common attacks.
- Don't ignore software updates - they contain patches that keep your device secure. Your organisation may manage updates, but if you're prompted to install any, make sure you do.
- Always lock your device when you're not using it. Use a PIN, password, or fingerprint to unlock a device if it is left unattended.
- Avoid downloading apps from unofficial app stores (like Google Play Store), which provide malware. Don't download apps from untrusted vendors and sources.

Use strong passwords

Attackers will try the most common passwords (e.g. password1), or use publicly available information to try and access your accounts. If successful, they can use this same password to access your other accounts.

- Create a strong and memorable password for important accounts, such as by using three random words. Avoid using predictable passwords, such as dates, family and pet names.
- Use a separate password for your work account. If an online account gets compromised, you don't want the attacker to also know your work password.
- If you write your passwords down, store them securely away from your device. Never reveal your password to anyone; your IT team or other provider will be able to reset it if necessary.
- Use two factor authentication (2FA) for important websites like banking and email. If you're given the option, 2FA provides a way of 'double checking' that you really are the person you are claiming to be when you're using online services.

If in doubt, call it out

- Reporting incidents promptly - usually to your IT team or line manager - can massively reduce the potential harm caused by cyber incidents.
- Cyber attacks can be difficult to spot, so don't hesitate to ask for further guidance or support when something feels suspicious or unusual.
- Report attacks as soon as possible - don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link), always report what's happened.
- Don't be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of people doing their jobs, doesn't work.

6

7

8

Cyber Essentials

- Helps you guard against the most common cyber threats & demonstrate your commitment to cyber security. Organisations should be Cyber Essentials accredited. Sign up www.cyberessentials.ncsc.gov.uk

Mail Check

- Free Platform for assessing email security compliance. It collects, processes & analyses DMARC reports from across the **public sector**

NCSC Exercise in a Box

- Free Service that helps you test your cyber maturity with testing and resilience plans

Web Check

- Free Service that helps you find & fix common vulnerabilities in UK **public sector websites**

Cyber Security Information Sharing Partnership (CISP)

- Joint industry & government initiative set up to exchange cyber threat information in a confidential & dynamic environment, increasing situational awareness & reducing the impact on UK business
- Once in CiSP join the maritime sector / modal specific nodes in order to interact & gain further insight

Utilise the Protective Domain Name System (PDNS)

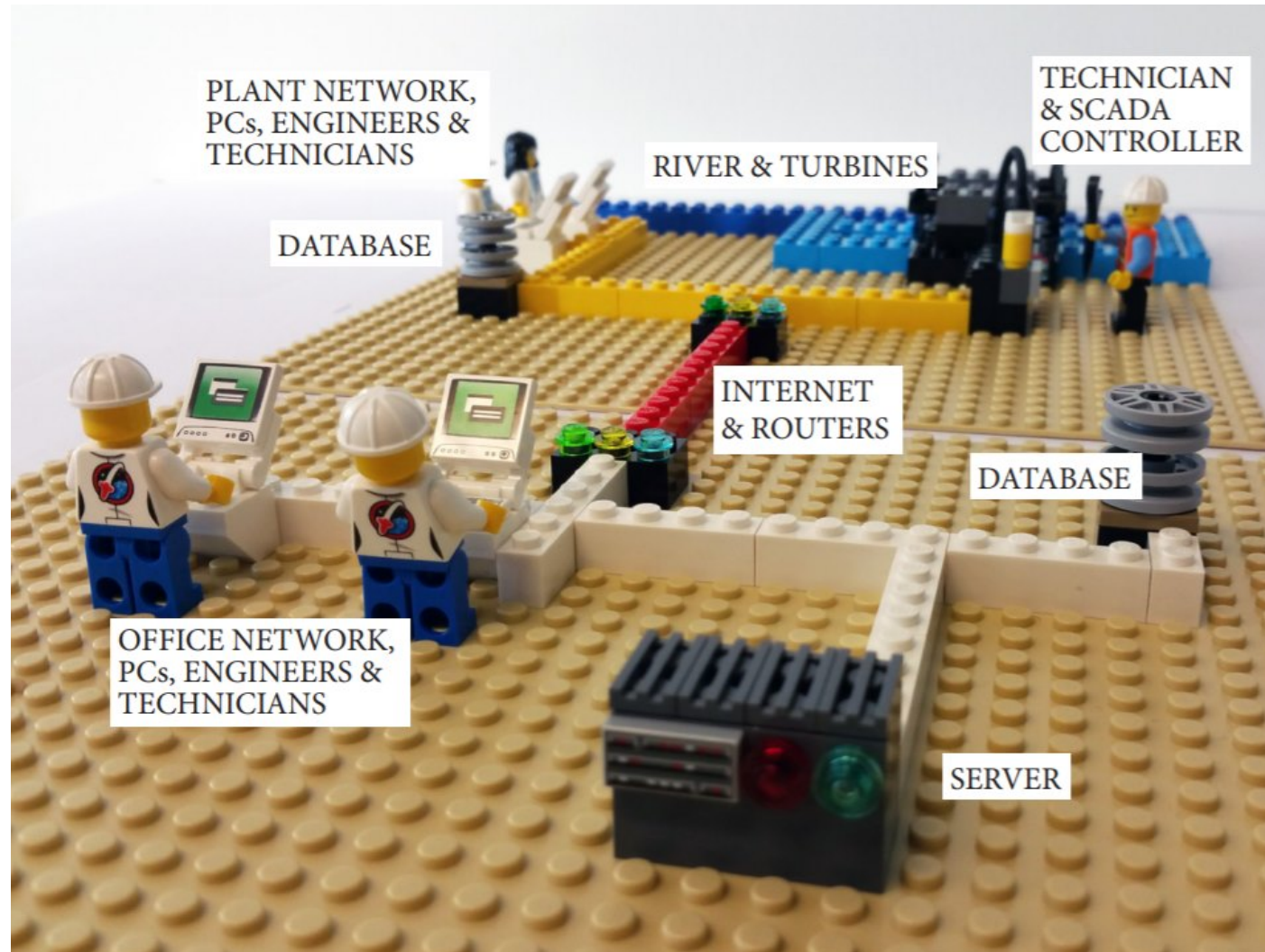
- Free reliable internet accessible DNS service for the public sector that protects users from threats posed by known malicious malware

Register for Cert-UK Network Reporting Service (CNR)

- Free service that scans for network abuse events & vulnerable network services on an organisation's Internet-facing services

DECISIONS AND DISRUPTIONS

A lego based table top exercise to challenge organisations response to Cyber Security



<https://sites.google.com/view/decisions-disruptions/>

The Consequences



- NotPetya - Ransomware
- 15% worlds shipping
- Stopped 76 port operations
- Rotterdam gridlocked
- Relied on WhatsApp
- \$200-300million cost
- Not the target!

PASSPHRASE NOT PASSWORD

The 25 worst passwords of 2018 ...

666666
Donald
1234567
123456
Password

123456789
12345678
12345
111111
Sunshine

Qwerty
Iloveyou
Princess
Admin
Welcome

Abc123
Fottball
123123
Monkey
654321

!@#\$%^&*
Aa123456
Password1
Qwerty123
Charlie

But how long does it take to crack these passwords?

QwErTy987123!

CoffeeTinyFish

CoffeeTinyFish#9

Don't use any information that may be easily worked out from social media content
e.g. maiden name; date / birth place; pets; football teams, etc...

To add complexity, convert letters to numbers and add special characters and use **THREE RANDOM WORDS**

For example
To add complexity
Or

LONDONBEACHMUSIC
LO7DO7B3ACHMUSIC
3redhousemonkeys!

References

Guidance documents from the Department of Transport for the maritime sector

- Note - Ports and Port systems guidance is in the process of being revised
- <https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice>
- <https://www.gov.uk/government/publications/ship-security-cyber-security-code-of-practice>

Useful data management guidance for protecting sensitive data

- <https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data>

All advice in this presentation is available on our website

- www.serocu.police.uk/staying-secure/

Get the latest reports from the National Cyber Security Centre

- Cyber Alerts and Advisories: www.ncsc.gov.uk/index/alerts-and-advisories
- Weekly Cyber Threat Report: www.ncsc.gov.uk/index/report

Thank you – Any questions?

Protect Team Email: cyberprotect@serocu.pnn.police.uk

To improve the products and services provided by Cyber Protect Officers, we welcome your feedback and ask that you complete a short survey.

To take you straight to this survey, please scan the adjacent smart code



Follow our social media for simple and practical advice on how to protect yourself from fraud and cybercrime



National Cyber Security Centre
a part of GCHQ

@SECyberprotect

SECyberprotect

SEROCU

Cyber Protect

South East ROCU

Cyber Protect

