Modern Policing & the Fight Against Cyber Crime

Presented By:

Sgt Phil Cobley

Regional Cyber Protect Coordinator
Regional Cyber Crime Unit
ERSOU

Who is this guy?

- Over 10 years experience in the Police
- Regional Cyber Protect Coordinator for ERSOU
- Previously Digital Forensics & Cyber Crime Investigations Manager
- Qualified Digital Forensics Practitioner in Computer and Mobile Examinations
- Certified in Information Security Management
- Currently studying BSc in Software Development (part time)
- Bedfordshire Police Force Practitioner Lead on Cyber Crime
- Guest Lecturer at several Universities in the region
- Member of the Cyber Security Centre at University of Hertfordshire
- Sat on the National ISO 17025 Standards Expert Network

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Eastern Region Special Operations Unit (ERSOU)

- Established back in 2010 as the Eastern ROCU
- Increase response to tackling threat of Organised Crime
  - *Identify*
  - *Disrupt*
  - *Dismantle*
- Provide Covert Policing Capability across Six Forces
- Some of our assets include:
  - *Regional Investigation Teams*
  - *Eastern Region Intelligence Unit (ERIU)*
  - *Regional Asset Recovery Team (RART)*
  - *Asset Confiscation Enforcement (ACE)*
  - *Regional Economic Crime Unit (RECU)*
  - *Regional Cyber Crime Unit (RCCU)*
  - *…and several more*

So what is Cyber Crime?

Cyber Crime in the UK is…

The adopted definition of Cyber Crime is:

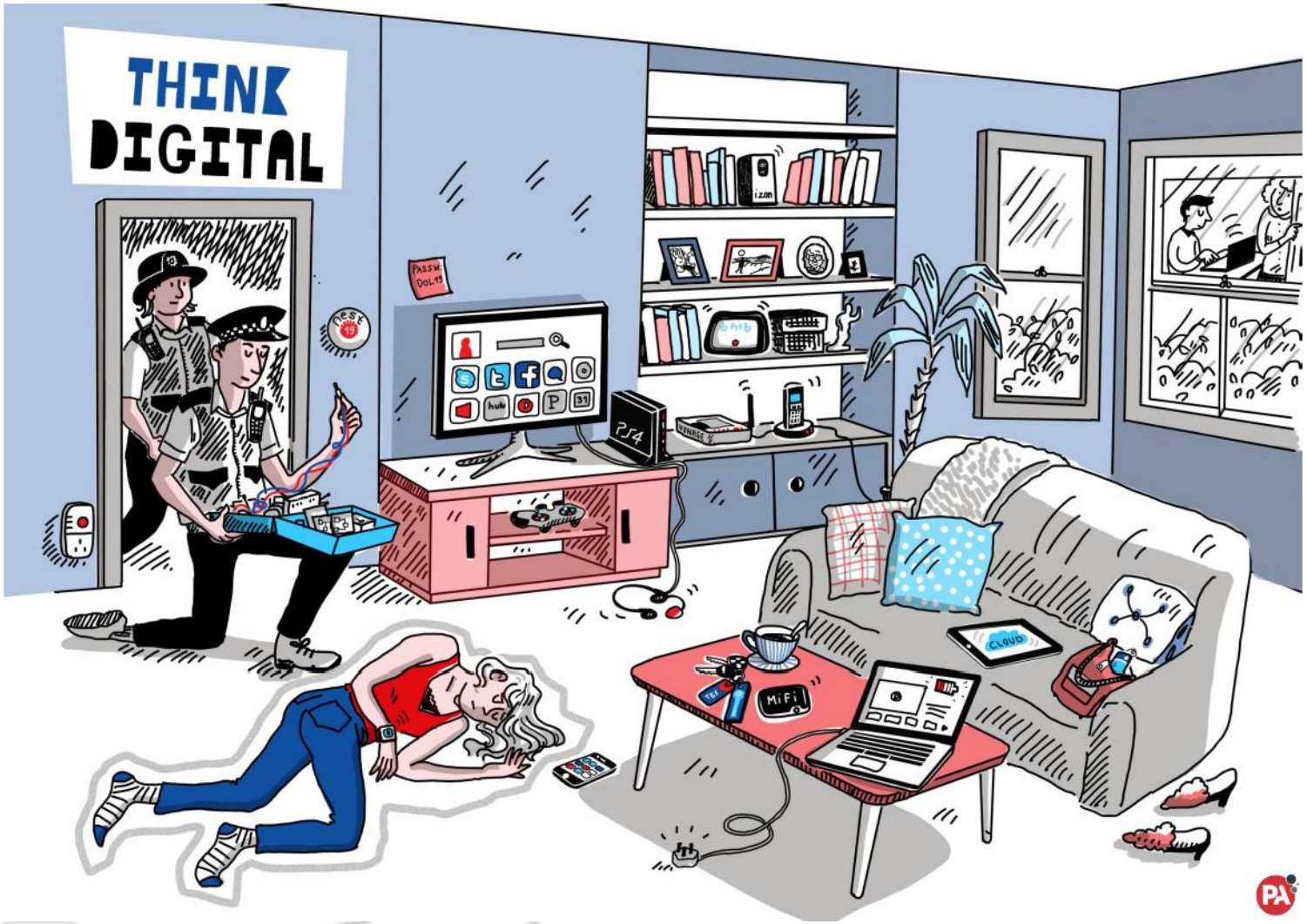
Cyber Dependent Crimes**,** where a digital system is the target as well as the means of attack. These include attacks on computer systems to disrupt IT infrastructure, and stealing data over a network using malware (the purpose of the data theft is usually to commit further crime).

Cyber Enabled Crimes. 'Existing' crimes that have been transformed in scale or form by their use of the Internet. The growth of the Internet has allowed these crimes to be carried out on an industrial scale.

The use of the Internet to facilitate drug dealing, people smuggling and many other 'traditional' crime types.

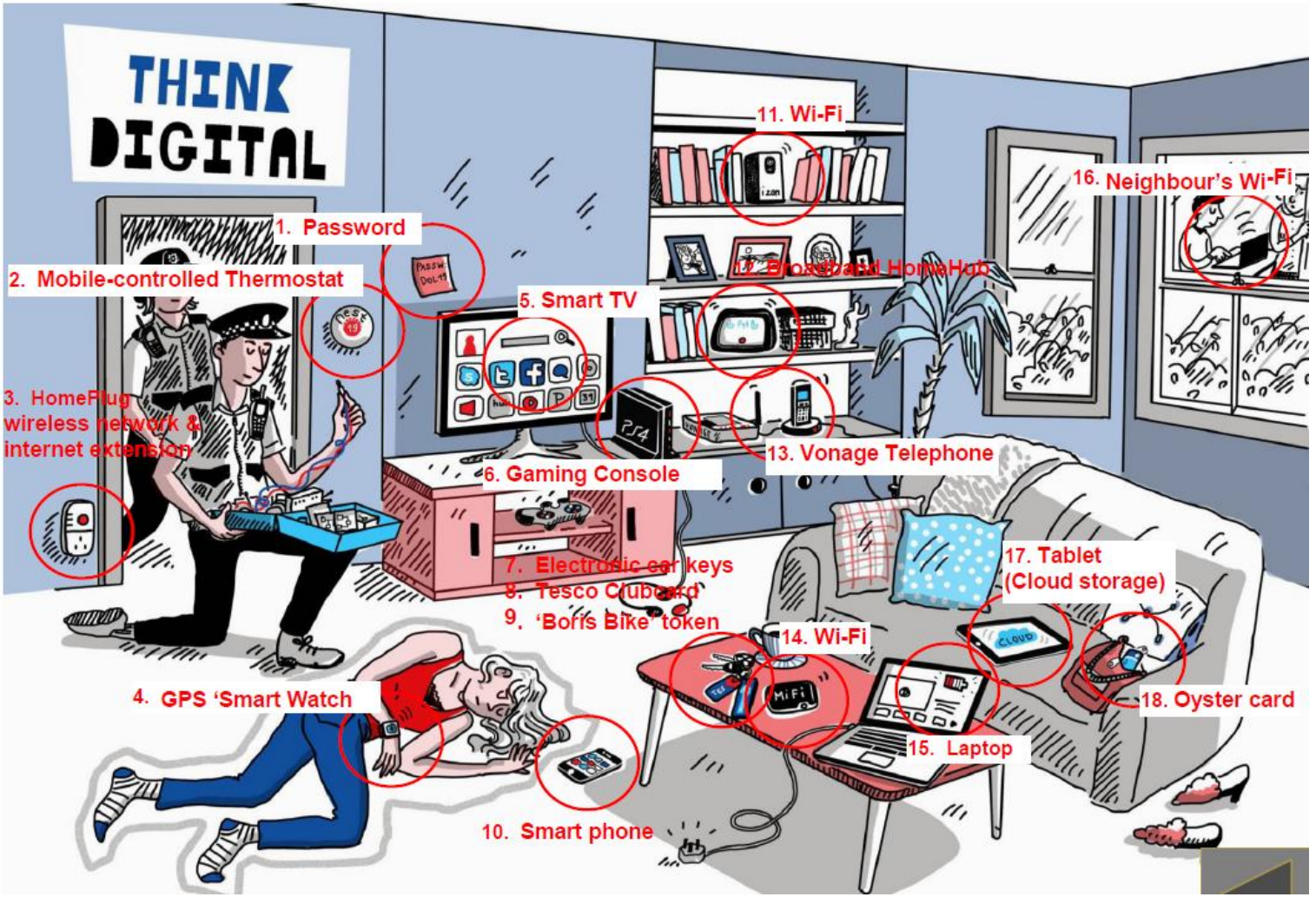
Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Think Digital – What are the lines of enquiry?



Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Think Digital – What are the lines of enquiry?



Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Which of these is a cyber threat?

POTENTIALLY ALL OF THEM!

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

So given we now know what a cyber crime is…

1969

So Cyber Crime - Is it really such a big deal?

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

We now live our lives online…

- UK has a 79% Penetration of Technology
- Affluent Country
- Cyber Security culture generally is poor
- Leads to the UK being a very attractive target
- Cost of Cyber Crime £27bn (Detica, 2011)

National Security Strategy Tier 1 threat

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

The Cost to Business…

The **2015** Information Breaches Survey reported that **90%** of large organisations and **74%** of small businesses had security breaches.

1) What is the average monetary loss for small businesses?

£75k - £311k

(Up from £65k - £115k in 2014)

2) What is the average monetary loss for large businesses?

£1.46m - £3.14m

(Up from £600k - £1.5m in 2014)

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

But we also know that it is easily preventable!!

GCHQ reported in 2014 that in terms of Cyber Crime…

80% is easily preventable

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

But what are some of the biggest threats?

- Insider Threat
- DDoS
- Social Engineering
- Malware
- Data Breach

But ultimately it depends on the business, how it is set up, the infrastructure and the policies and procedures

What is social engineering?

"When talking about online safety and security, 'social engineering' means the act of manipulating or tricking people into certain actions including divulging personal or financial information … a kind of confidence trick. Social engineering exploits human nature and often plays on victims' willingness to be helpful, or please others. It is a factor in many types of fraud."

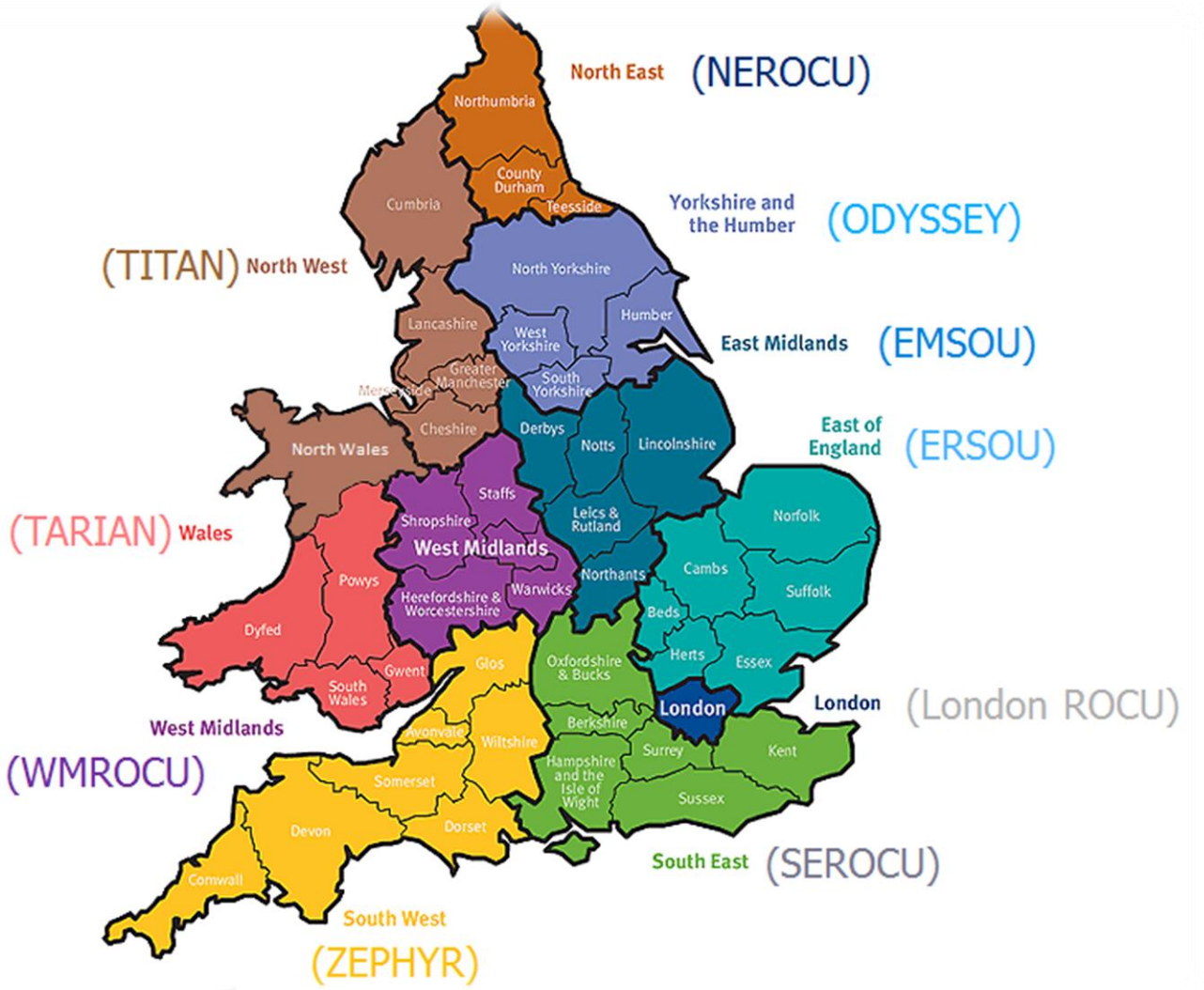
- Get Safe Online, Jan 2016

Some examples of social engineering

- Fraudulent emails encouraging you to follow a link or open an attachment – (*Phishing*)
- Fraudulent phone call asking you to confirm details – (*Vishing*)
- Being advised to hand over payments cards etc to a courier – (*Courier Fraud*)
- Fraudulent phone call requesting remote access (i.e. Microsoft Scam)
- USB/DVD left lying around or given to you which contains Malware – (*Baiting*)
- Fake social network profiles trying to be your friend
- Online Dating Scams – (*Romance Fraud*)

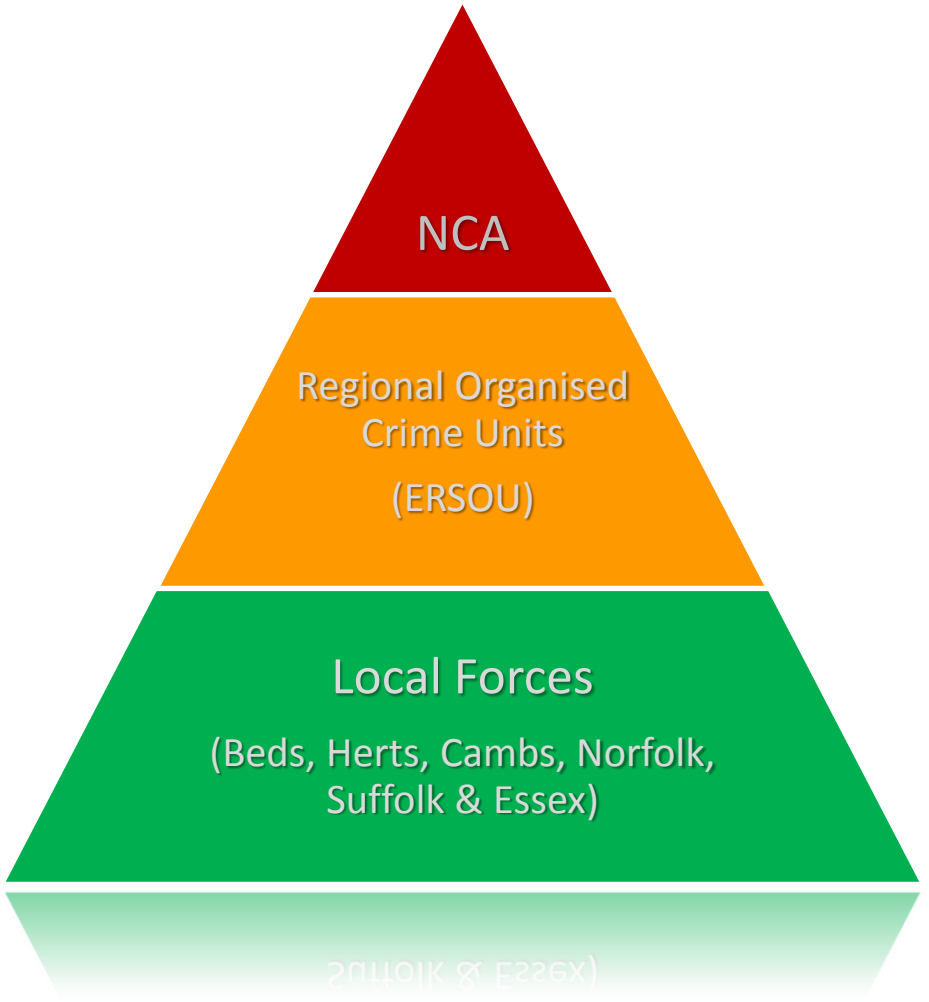
Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

So how has Law Enforcement adapted…?



Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

The National, Regional and Local Picture…



Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

The Four ‘P’ Strategy

Prepare

Protect

Prevent

Pursue

Peel's First Principle

"The basic mission for which the police exist is to prevent crime and disorder"

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

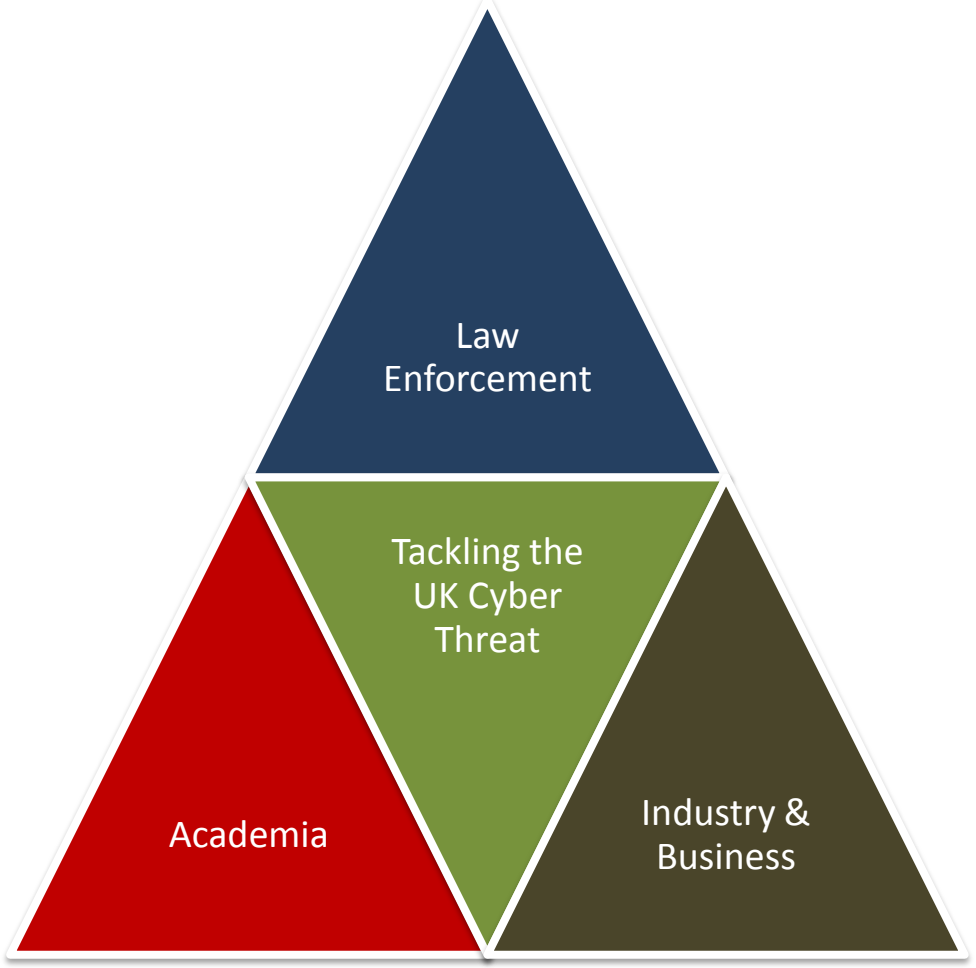
Moving our Focus to “Protect & Prevent”

- Report recommends “***a greater focus on protect against and preparing for cyber crime***” not just trying to pursue criminals.

- There is a clear ***need for more help*** to protect, prepare and educate SMEs

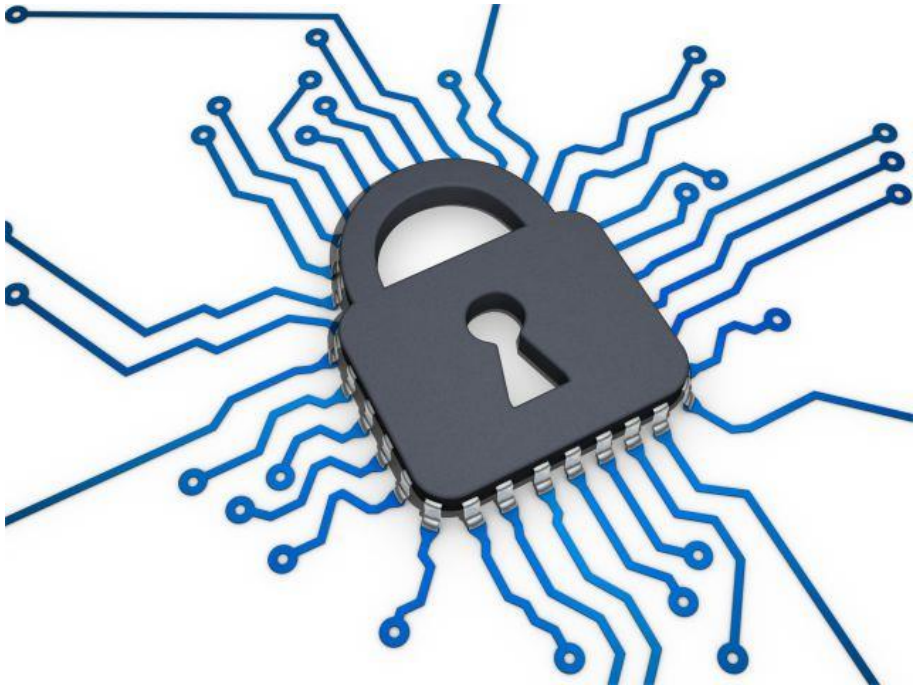
- Constant requirement to ***review incidents, highlight lessons learned and share these experiences***

The Protect Network is here to realise that 80% Figure!



Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Partnering with Business & Industry

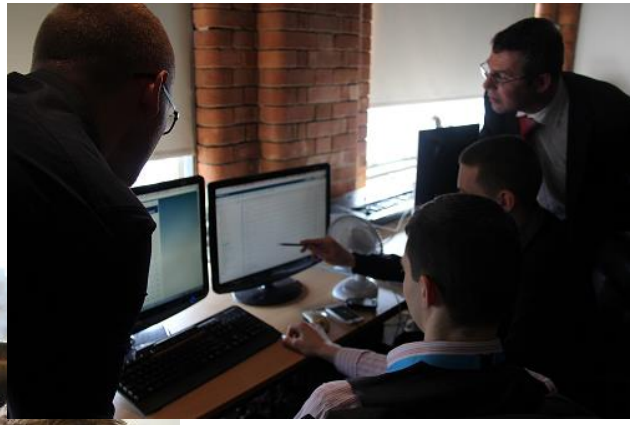


Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Partnering with Universities

Anglia Ruskin University
Cambridge & Chelmsford

University of Hertfordshire



UEA
University of East Anglia

UCS
University Campus Suffolk

University of Bedfordshire

UNIVERSITY OF CAMBRIDGE

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Partnering with the BCS

COMPUTING AT SCHOOL
EDUCATE · ENGAGE · ENCOURAGE
Part of BCS, The Chartered Institute for IT

bcs

Cranfield UNIVERSITY

BCS (Bedford Branch) School Challenge 2016

A competition to showcase how computing is being developed in schools, how it is engaging pupils and enabling them for computing futures.

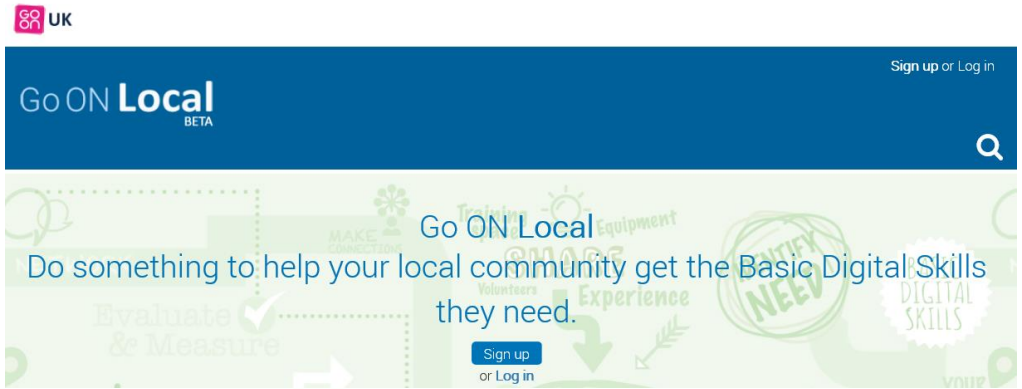
Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

National Volunteering Programme

GO ON UK

GET SAFE ONLINE

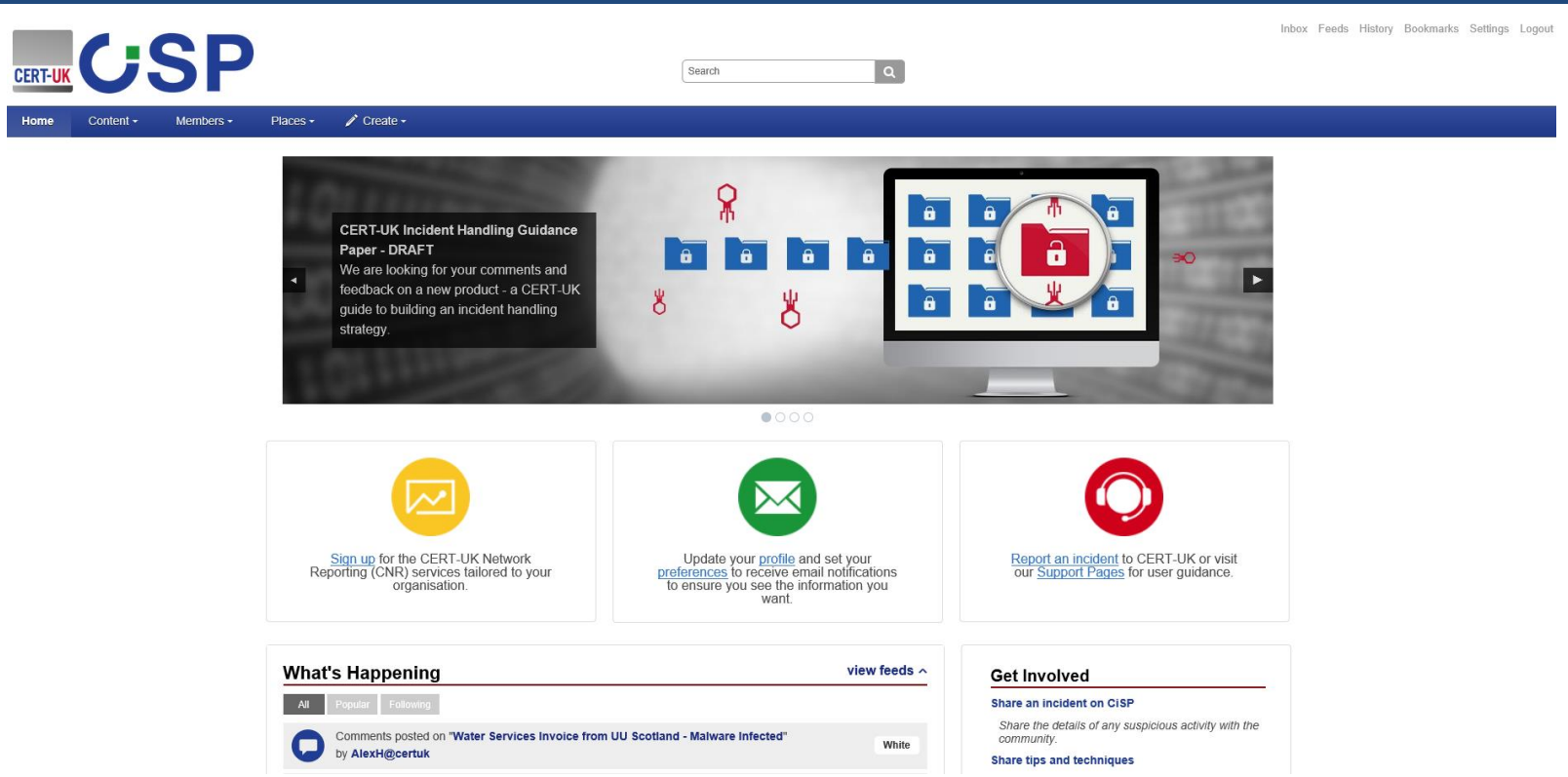
Get Safe Online



CYBER STREETWISE

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

CiSP – Cyber Information Sharing Partnership



CERT-UK

www.cert.gov.uk/cisp

enquiries@cert.gov.uk

@CERT_UK

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

CiSP – Our Internet – Our Community – Our Responsibility

CiSP

A CATALYST FOR COLLABORATION

So how can you protect yourselves?

- Cultural Change
- Accept that it is "*When*" not "*If*"
- Cyber & Information Security is *not always about technology*
- 80% preventable with *very simple steps*
- Always consider the home life/work life blend of good practice

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Firstly, answer a few questions…

- Do you know the value of your data?
- Do you know where your data is stored?
- Who has access to that data? (suppliers/providers/employees)
- Do you really know your employees? (Proper vetting, single point of failure?)
- Do you have backups & do they work?
- What would you do if you lost all your data tonight?
- Reputational Damage/IP/Trust…what if these were affected?
- Do you have suitable business continuity and disaster recovery in place?
- Do you know what your responsibilities are if you have a data breach?
- What is your incident response plan?

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Some Simple Tips & Tricks: Passwords

Time it takes to crack*:

“password”

Instantaneous

“P@s2W0#D”

9 hours

“P@s2W0#D72”

6 years

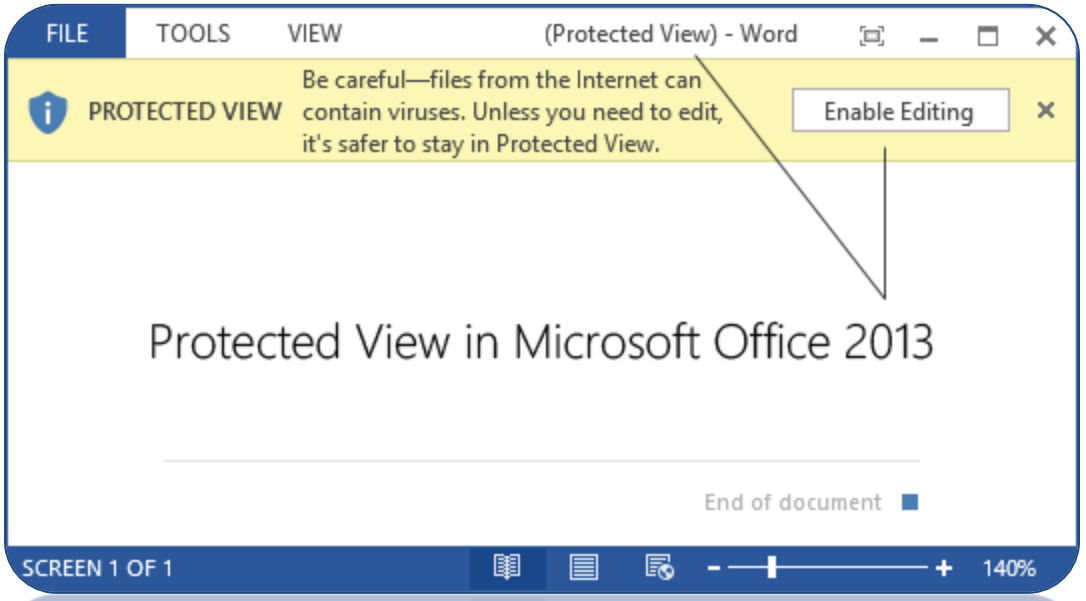
“humptydumptysatonawall”

11 trillion years

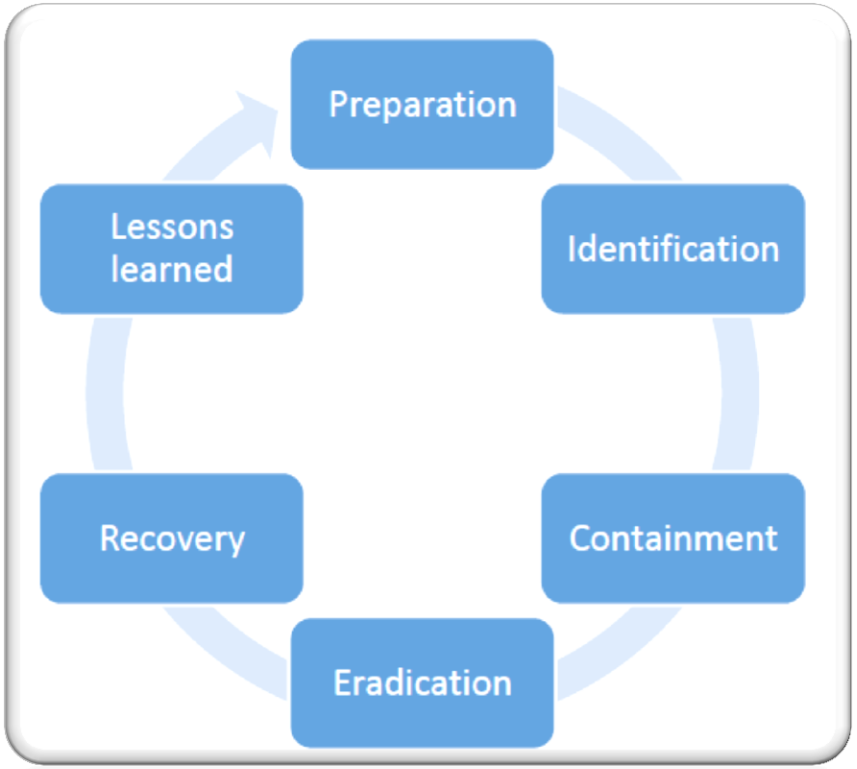
** Source: https://howsecureismypassword.net/*

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Some Simple Tips & Tricks: Macros & Protected View



Some Simple Tips & Tricks: Incident Response



Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Some Simple Tips & Tricks: Training & Awareness

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Some Simple Tips & Tricks: Be Clever with Security Questions

- What is the name of your first pet?
- What is your mother's maiden name?
- What was the name of your first school?
- What is the name of your favourite band?
- What is your father's middle name?
- …and so forth…

Eastern Region Special Operations Unit
TACKLING ORGANISED CRIME

Security questions – I found some interesting alternatives…

- What is the name of your least favourite child?
- In which park did you first get drunk on cheap alcohol as a teenager?
- What sports team do you fetishize to avoid meaningful discussion with others?
- In what year did you abandon your dreams?
- What is the nickname you always wanted, but never had?
- What is the nickname you always had, but never wanted?
- When did you stop trying?

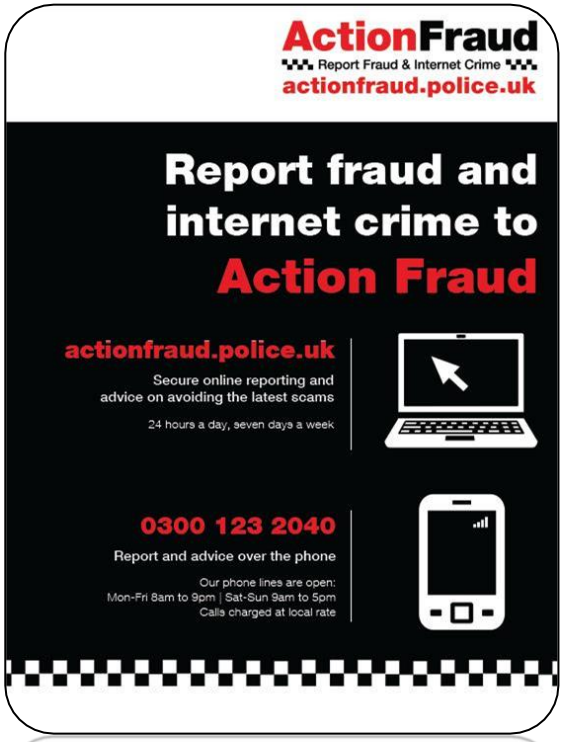
Who do I Contact?

- Action Fraud – **0300 123 2040**

- Urgent Incidents – **999** or **101** (local Force response)
- Non urgent incidents – **101** / **Action Fraud**
- Non urgent in office hours – **Local Force Cyber Crime Unit** (email me for details)

- *Regional Unit will pick up incidents/cases through a tasking process that local Forces initiate*

- *Action Fraud will disseminate cases and investigations across to Forces following research and analysis of information provided*



Did anyone work out the significance?

1969

Thank you!

Sergeant Phil Cobley
Regional Cyber Protect Coordinator
Regional Cyber Crime Unit
Eastern Region Special Operations Unit (ERSOU)

(+44) 07507 684387
phil.cobley@ersou.pnn.police.uk