BEDFORDSHIRE POLICE
Protecting People and Fighting Crime
Together

BEDFORDSHIRE POLICE

Cybercrime

Digital Forensics & Investigations Unit

“The Challenge for us All”

D/Supt Jon Gilbert

14/09/2015 - v 1.0

We live our lives online

3bn people will be using the internet worldwide by 2016 and by the end of the year, networked devices will outnumber people by six to one

On average each household has 3 internet enabled devices and 2/5 adults have smart phones

8% of GDP generated through the internet economy

£121bn in 2010 with Household annual retail sales worth £2.6bn with 30% year on year growth

Estimated cost of Cyber Crime- £27billion – 2% GDP (Detica 2011)

£21 billion to business

£2.2 billion to government

£3.1 billion to ‘Jo Public’

44m cyber attacks in 2011 in UK

National Security Strategy Tier 1 threat

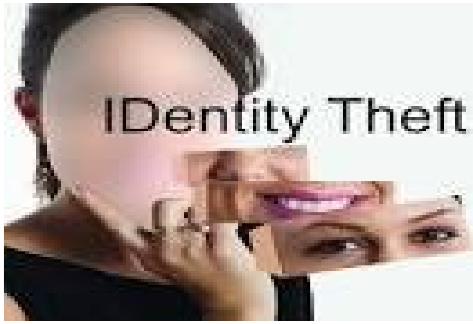
Measuring the Cost of Cyber Crime

(Anderson et al Feb 2013)

‘Cyber is now the typical volume crime in the UK’

The Economic Cost of Cyber Crime up to $500 billion
(McAfee July 2013)

Crime Survey for England & Wales 2012



One in three adults suffered online

Crime in the previous 12 months

One in five suffered off line crime

Federation of Small Business (21/05/12)

41% of members suffered cyber crime

in the last 12 months cost of £800m

20% had taken no steps to protect themselves

Current Threats/Vulnerabilities

Threats

Identity Fraud

(Staff)

PBX Fraud

DDOS

Insider Fraud
(Bribery and corruption/infiltration)

Invoice Fraud

Payment Card
Card not present & Fuel Card compromise

Vulnerabilities

Social Engineering

(Customers)

Consumer Behaviour

Bring Your Own Devices

Agile Working
Public/Unsecured Wifi

GCHQ report…

80% easily preventable

What does this mean?

This is the new SOC, the new protest crime, the new volume crime

Mrs Miggins, 1 Acacia Avenue…. to big business and national security

Crime not so much down, just changing… in a way not accounted for in crime stats

$C_5H_5N_5$ $C_5H_5N_5O$ $C_4H_5N_3O$ $C_5H_5N_2O_2$ PO_4 C_5H_9O

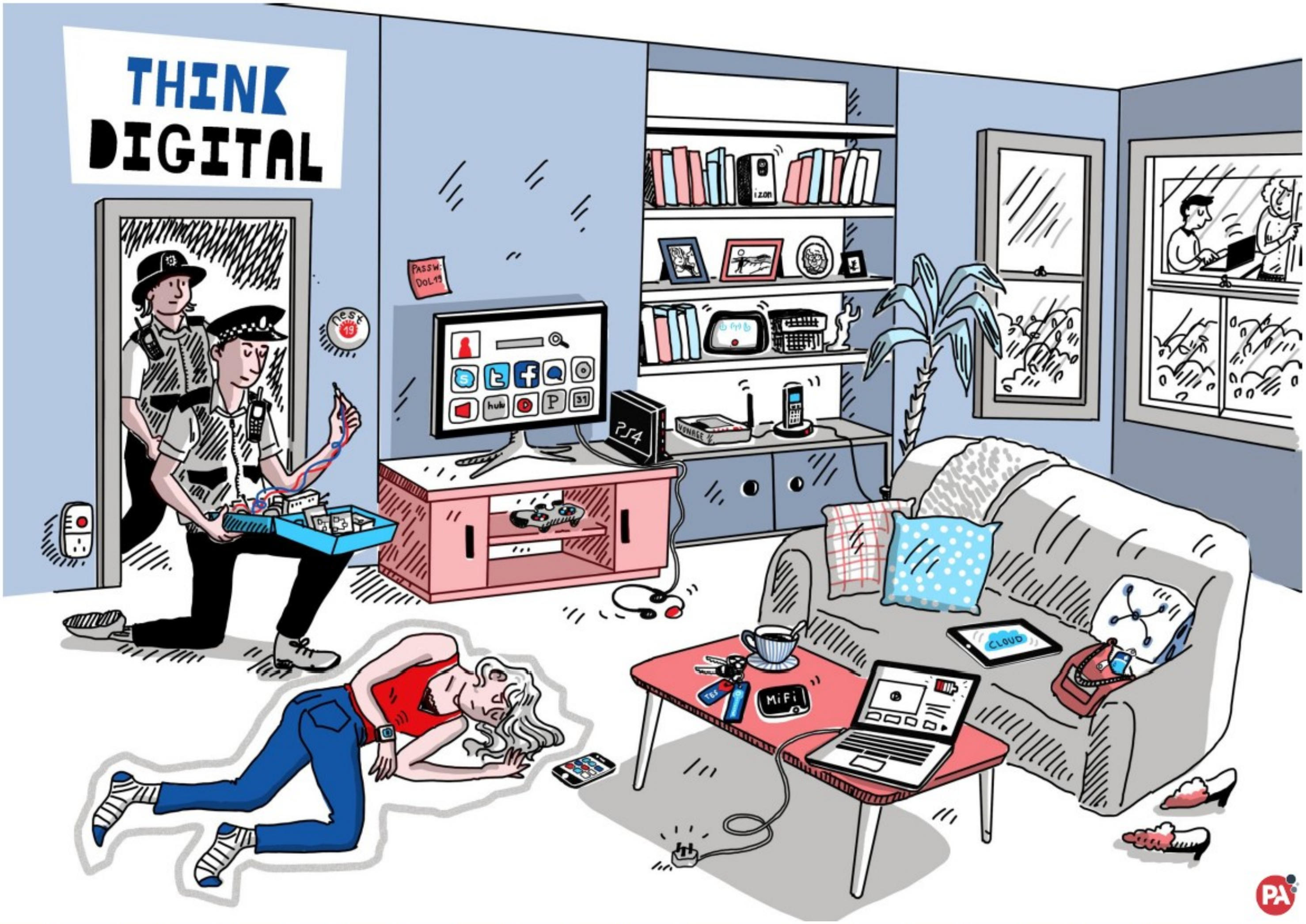
Chemical Formula for DNA

DNA

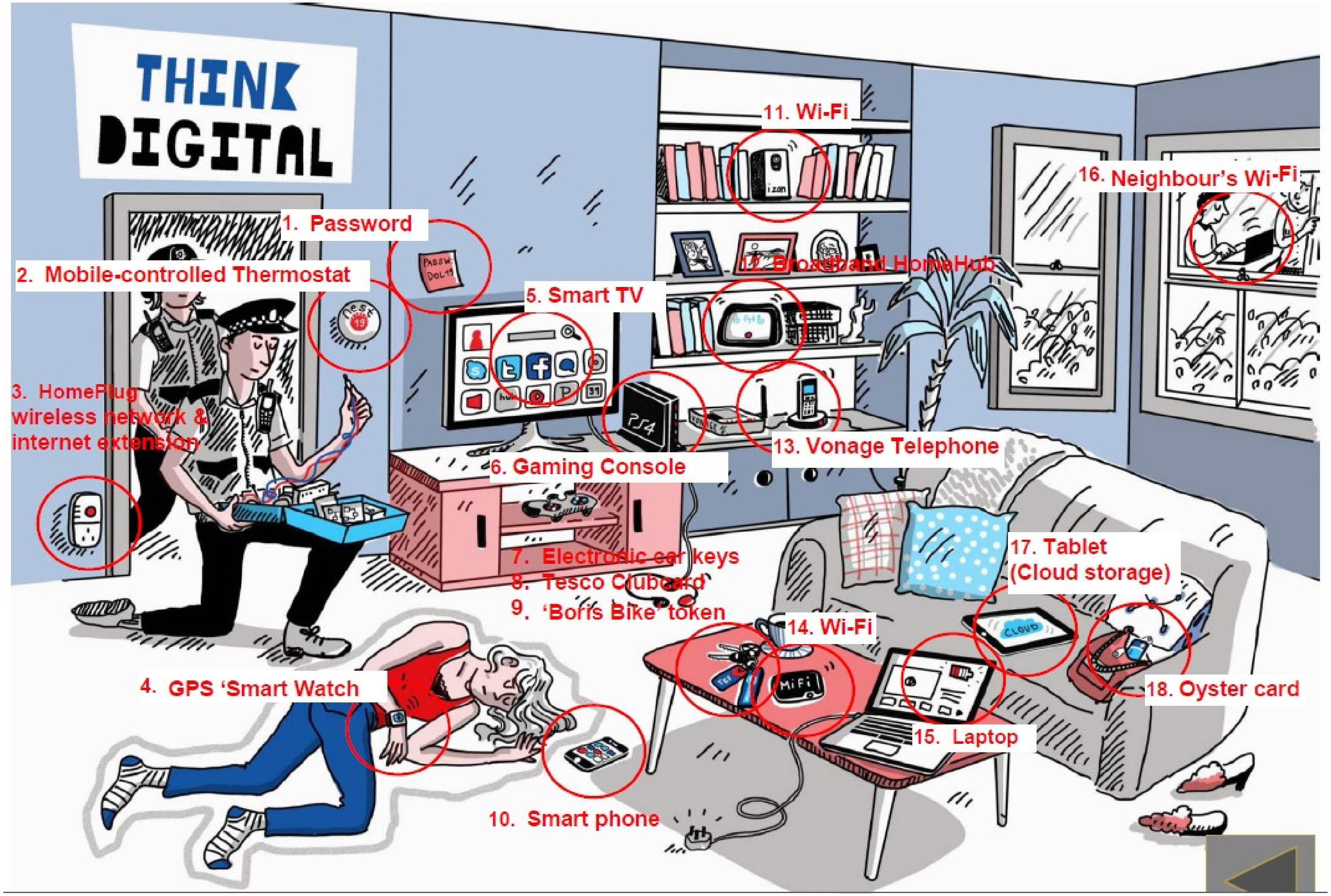
- 25 years ago a new concept
- Had improved our knowledge, understanding and working practices
- Not everyone needs to know the Chemical Formula, or how to extract it from a crime scene sample, but we all have to understand it’s implications in criminal investigations

Think Digital…

BEDFORDSHIRE POLICE
Protecting People and Fighting Crime
Together



Think Digital…answered…



How old is a cyber criminal

BEDFORDSHIRE POLICE
Protecting People and Fighting Crime
Together

I'll hazard I can do more damage on my laptop sitting in my pajamas
before my first cup of Earl Grey than you can do in a year in the field.

A Cyber-crime is a crime

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.

Government Response

- Governance & Mandation
- Strategic lead for UK Law Enforcement
- Formation of National Infrastructure – NCA & ROCU Cyber Responses
- New International Reach
- Uplift in capability and capacity
- National “Minimum standards”

Overarching Strategy (Cyber)

- *PURSUE*
  - Prosecute & disrupt criminals engaged in cyber crime
- *PREVENT*
  - Prevent people from engaging in cyber crime
- *PROTECT*
  - Increase protection from cyber criminals
- *PREPARE*
  - Reduce the impact of cyber crime when it occurs

Peel’s First Principle

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

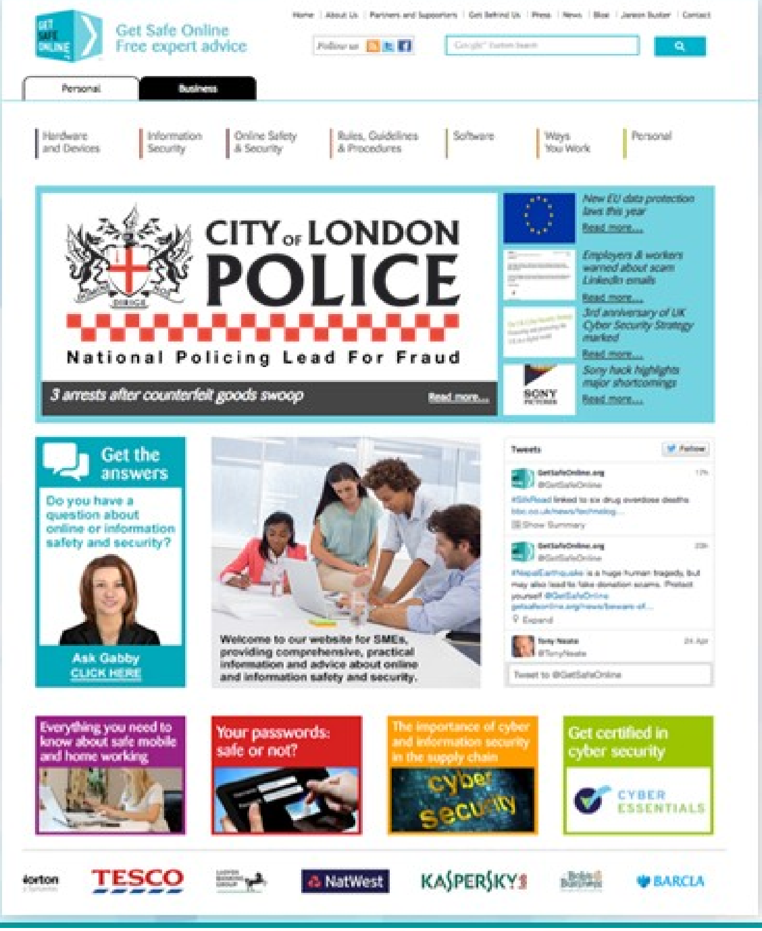
Resources – Get Safe Online

BEDFORDSHIRE POLICE

Business website

- Comprehensive site to advise businesses on staying safe online
- Latest scams & advice

Internet Safety
Starts with
you.



3 arrests after counterfeit goods swoop Read more...

New EU data protection laws this year Read more...

Employers & workers warned about scam LinkedIn emails Read more...

3rd anniversary of UK Cyber Security Strategy marked Read more...

Sony hack highlights major shortcomings Read more...

Get the answers

Do you have a question about online or information safety and security?

Ask Gabby CLICK HERE

Welcome to our website for SMEs, providing comprehensive, practical information and advice about online and information safety and security.

GetSafeOnline.org @GetSafeOnline 17h
#SilkRoad linked to six drug overdose deaths bbc.co.uk/news/technolog...
Show Summary

GetSafeOnline.org @GetSafeOnline 23h
#NepalEarthquake is a huge human tragedy, but may also lead to fake donation scams. Protect yourself @GetSafeOnline getsafeonline.org/news/beware-of...
Expand

Tony Neate @TonyNeate 24 Apr

Tweet to @GetSafeOnline

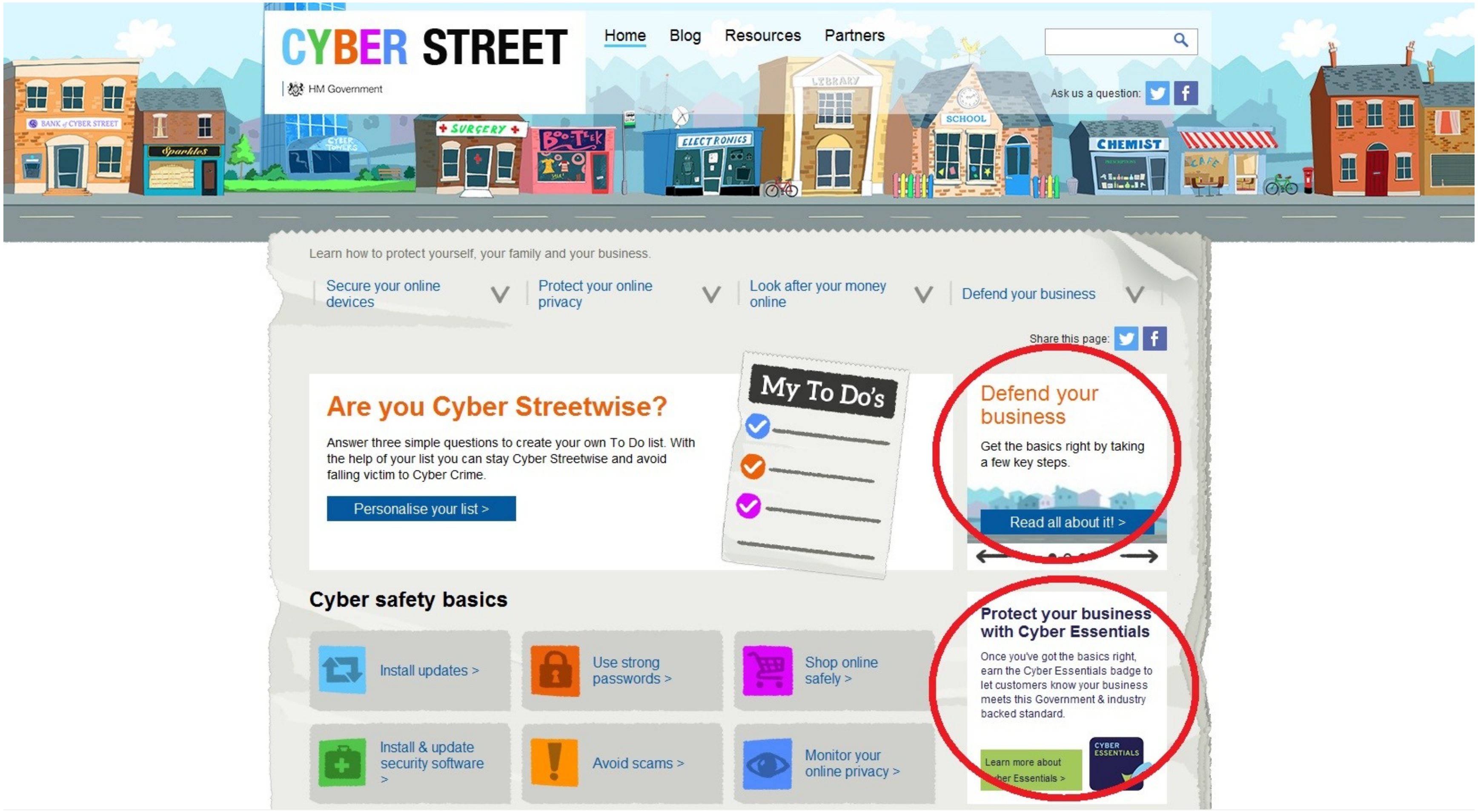
Everything you need to know about safe mobile and home working

Your passwords: safe or not?

The importance of cyber and information security in the supply chain

Get certified in cyber security

Resources – Cyber Street



Learn how to protect yourself, your family and your business.

Secure your online devices ∨ | Protect your online privacy ∨ | Look after your money online ∨ | Defend your business ∨

Share this page:

Are you Cyber Streetwise?

Answer three simple questions to create your own To Do list. With the help of your list you can stay Cyber Streetwise and avoid falling victim to Cyber Crime.

Personalise your list >

Defend your business

Get the basics right by taking a few key steps.

Read all about it! >

Cyber safety basics

- Install updates >
- Use strong passwords >
- Shop online safely >
- Install & update security software >
- Avoid scams >
- Monitor your online privacy >

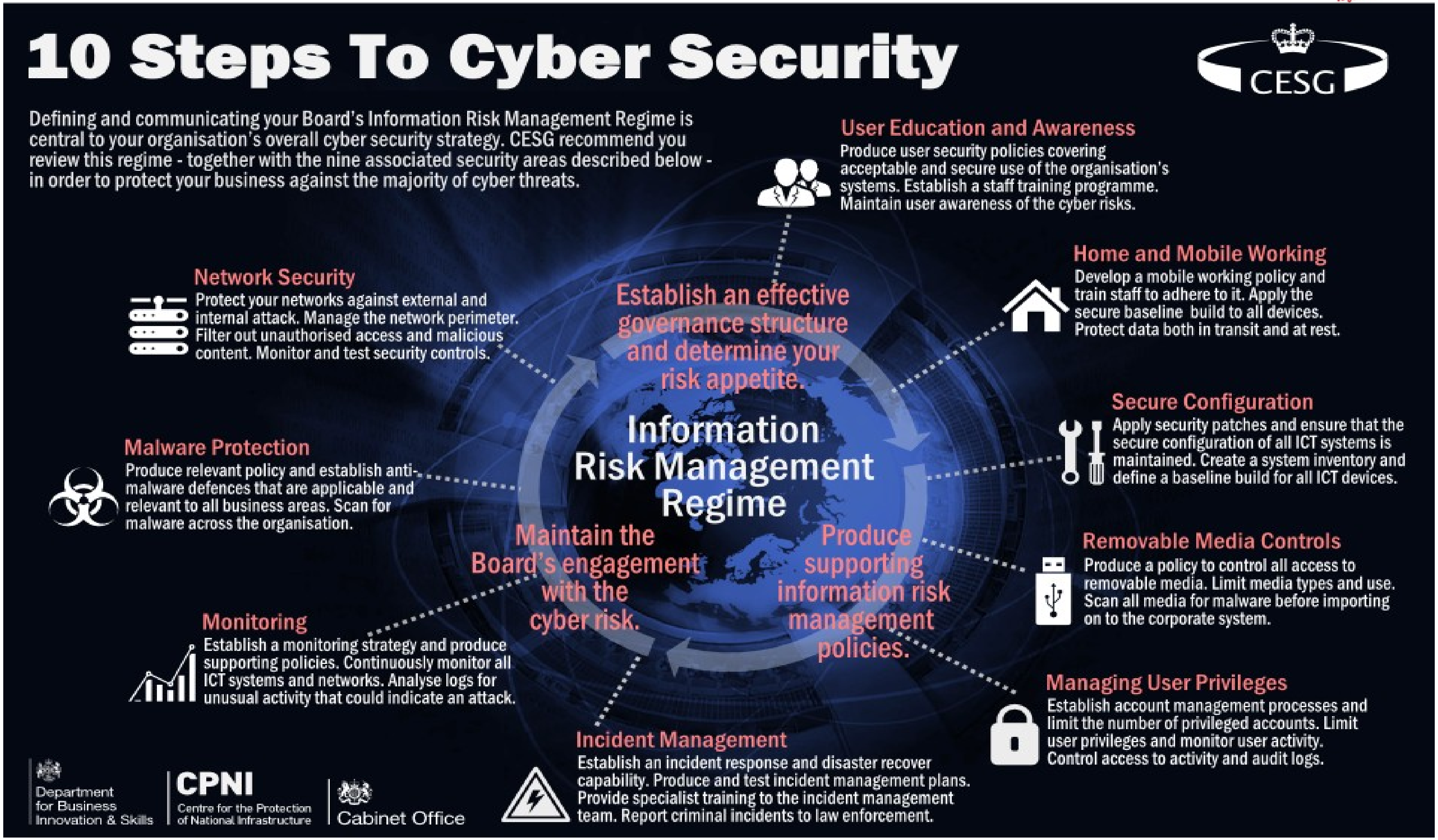
Protect your business with Cyber Essentials

Once you've got the basics right, earn the Cyber Essentials badge to let customers know your business meets this Government & industry backed standard.

Learn more about Cyber Essentials >

CYBER ESSENTIALS

Resources – Cyber Essentials



10 Steps To Cyber Security

CESG

Defining and communicating your Board's Information Risk Management Regime is central to your organisation's overall cyber security strategy. CESG recommend you review this regime - together with the nine associated security areas described below - in order to protect your business against the majority of cyber threats.

Information Risk Management Regime

Establish an effective governance structure and determine your risk appetite.

Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

User Education and Awareness
Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks.

Home and Mobile Working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.

Secure Configuration
Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.

Removable Media Controls
Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to the corporate system.

Managing User Privileges
Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident Management
Establish an incident response and disaster recover capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.

Malware Protection
Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.

Network Security
Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.

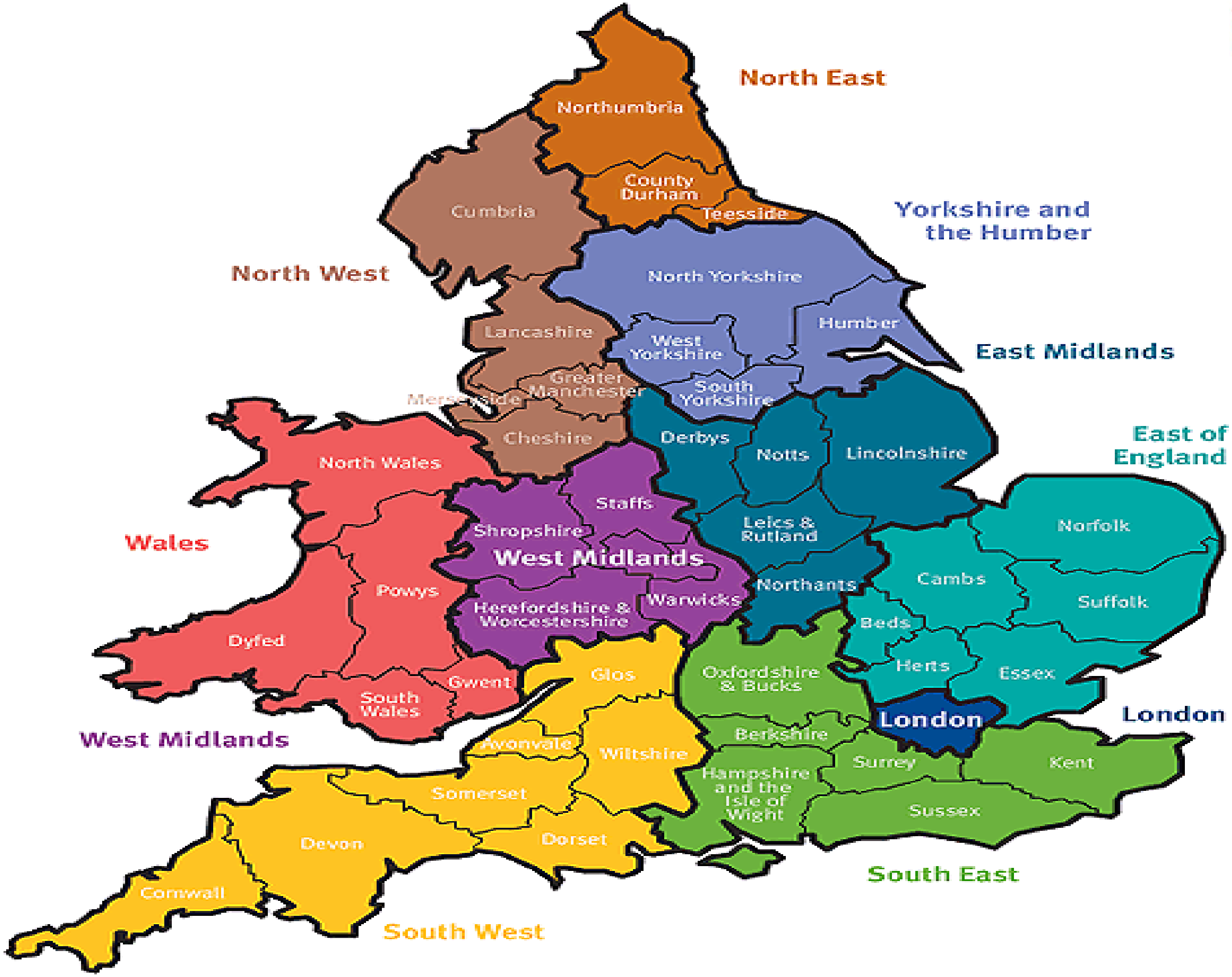
Department for Business Innovation & Skills

CPNI
Centre for the Protection of National Infrastructure

Cabinet Office

Regional Network

BEDFORDSHIRE POLICE
Protecting People and Fighting Crime
Together



Regional Focus

- Links into National Infrastructure
- Regional Cyber Information Sharing Platform (CISP)
- Trust Group incorporating Business/Academia
- Cyber Regional User Group
- RTTCG Tasked Operations/Service Level Agreement

Strategic Policing Requirement

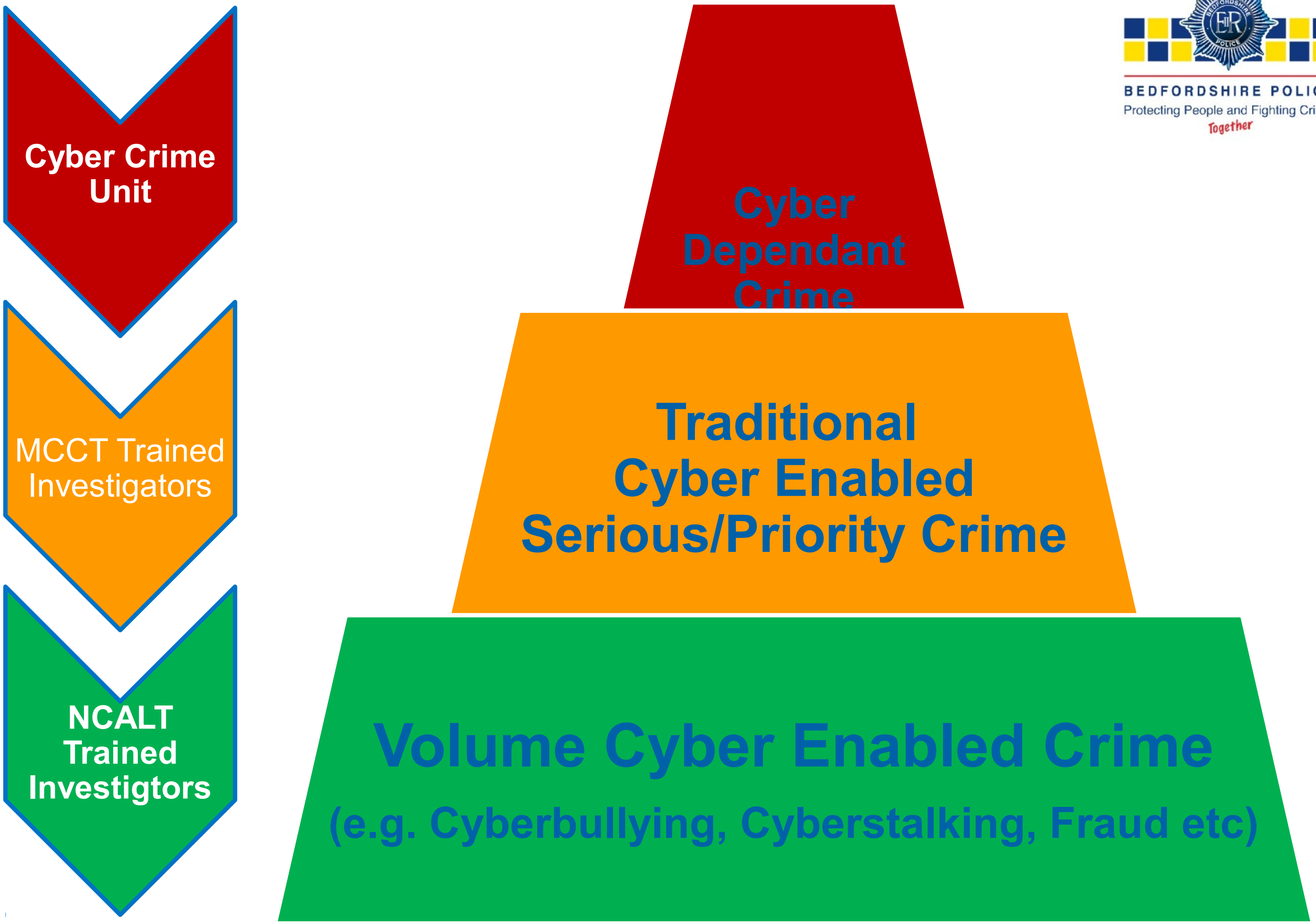
Five Threats Identified of which Cybercrime is one:

- A large-scale cyber incident.
- Terrorism.
- Other civil emergencies.
- Threats to public order or public safety.

Response Required: PCCs and CCs must demonstrate that they have taken into account the need for appropriate capacity to respond adequately to a major cyber incident through the maintenance of public order and supporting the overall incident management and response, recognising that the police response to cyber-related threats needs to develop further.

Bedfordshire Vision

- NCALT/NCALT + (Minimum Standard)
- Mainstream Cyber Crime Training
- Dedicated Force Cyber Hub designed to:
  -Advise, guide, support & own investigations (as appropriate)
- Close gaps in accepted National standards
- Future opportunities/Increased capabilities



Cyber Crime Unit

MCCT Trained Investigators

NCALT Trained Investigtors

Cyber Dependant Crime

Traditional Cyber Enabled Serious/Priority Crime

Volume Cyber Enabled Crime

(e.g. Cyberbullying, Cyberstalking, Fraud etc)

The Future

- Working together with Academia, Business & other partners
- Design of “Flagship” Cyber courses & accreditations
- Academic Research to real world cyber issues
- Police Knowledge Fund application
- Effective Horizon Scanning
- Student Partnerships
- Cyber Specials/Volunteers
- Incorporation of Cyber as Business as usual

Questions?

T/Det Supt Jon Gilbert
Force Cyber lead
01234 842803
07990 790662
jon.gilbert@bedfordshire.pnn.police.uk