

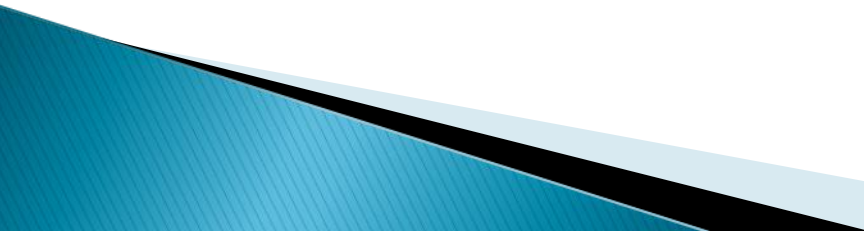
# *Zephyr* RCCU

---

South West  
Regional Cyber Crime Unit



# WHO ARE WE?

- ▶ One of nine RCCUs established in Jan 2014 to cover England and Wales
  - ▶ All sit within the nine ROCUs (South West - Zephyr)
  - ▶ Small unit but expanding with links to regional and national Law Enforcement as well as Government Departments, academia and industry
  - ▶ Focussed on dealing with serious incidents of cyber crime within the SW region
  - ▶ Expectation includes increasing cyber awareness across partners and creating local partnerships – Championing the use of (CiSP) Cyber Security Information Sharing Partnership
  - ▶ Force/Region/National and International
- 

# HOW?

Delivery against the 4 P's Serious and Organised Crime Strategy

- **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

# WHAT IS CYBER CRIME?

ACPO/NPCC defines as, *'The use of networked computers or internet technology to commit or facilitate the commission of crime'*.

Three fold categorisation dividing cyber crime into:

- ▶ 'Pure' online crimes where a digital system is the target as well as the means of attack. Includes attacks to disrupt IT infrastructure, exfiltration of data, the compromising of data integrity and making data unavailable
- ▶ 'Existing' crime that has been transformed in scale or form by the use of the internet. The growth of the internet has allowed crime to be carried out on an industrial scale
- ▶ Use of the internet to facilitate drug dealing, people smuggling and other traditional crime types

# Some stats....

- 81% of large organisations and 60% of small organisations reported a security breach (reduced slightly), although...
- Severity and impact has increased...the worst breaches averaging at £65k - £115k for small organisations and between £600k - £1.15m for large.
- 2014 saw more than 1,500 significant data breaches – global companies losing hundreds of millions of user details, sometimes including credit card and bank account details
- Credit card details with CVV being sold for as little as \$1 on black market exchanges
- Crime rate in England and Wales more than doubled to 11.6 million offences – primarily because of the inclusion of 5.1m incidents of online fraud and 2.5m incidents of cybercrime
- More than 70% of fraud is now committed online
- 2013 McAfee estimated Economic Cost of Cyber crime globally as \$500bn
- *Cyber Security identified as a Tier 1 threat to the UK, alongside Terrorism, War and Natural Disaster*
- *GCHQ report - 80% cyber crime preventable*

# What are we seeing in the SW RCCU?

- ▶ DRIDEX/SHIFU - This is banking malware, primarily linked to word documents. When opened it advises you to 'enable macros' (macros basically automate frequently-used tasks). It then waits until a person visits a banking website and steals login details. This is then used to move money.
- ▶ RANSOMWARE - Malware such as Cryptolocker and Cryptowall. These are executable files that are hidden as .pdf files. When opened they encrypt files on a network. A 'ransom' is then requested, usually payable in Bitcoin, to de-encrypt the files.
- ▶ SPEAR-PHISHING - Targeted attacks by e-mail that may entice you to a website or be the delivery mechanism for malware. These can be very familiar in tone or be 'spoofed' e-mailed addresses from clients or suppliers with invoices attached.
- ▶ NETWORK INTRUSION – targeting businesses and public authorities
- ▶ DDOS - Organised Crime Groups and kids!
- ▶ 'Spoofed' websites.

# The Attraction?

## Traditional Crime

- ▶ Presence at the crime scene
- ▶ One offence at a time
- ▶ High risk/low reward
- ▶ Local enquiries
- ▶ Victim reports to police

## Cyber Crime

- ▶ Remote from the crime scene
- ▶ Multiple offences at once
- ▶ Low risk/High reward
- ▶ International enquiries
- ▶ Victim reputation

**PREVENTION IS  
BETTER THAN  
CURE.....**

# 10 Steps To Cyber Security



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.

## 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.



Establish an effective governance structure and determine your risk appetite.

**Information Risk Management Regime**

Maintain the Board's engagement with the cyber risk.

Produce supporting information risk management policies.

## 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.



## 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.



## 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.



## 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.







Search bar with a magnifying glass icon, a Twitter icon, and a RSS icon.

Home > **Cyber-security Information Sharing Partnership (CiSP)**

# Cyber-security Information Sharing Partnership (CiSP)



A CATALYST FOR COLLABORATION

The Cyber-security Information Sharing Partnership (CiSP), part of CERT-UK, is a joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business.

CiSP allows members from across sectors and organisations to exchange cyber threat information in real time, on a secure and dynamic environment, whilst operating within a framework that protects the confidentiality of shared information.

CiSP members are also able to receive [network monitoring reports](#). This free service allows users to receive tailored feeds of information from CERT-UK covering any malicious activity that we see on your network.

Users can sign up for this service when they join CiSP or register your interest and a member of the team will get back to you when you have the necessary information.



**PREVENTION IS  
BETTER THAN  
CURE.....**

10 Steps to Cyber Security (from CERT UK)

<https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility>

Critical Security Controls guidance (20 steps)

<http://www.cpni.gov.uk?advice/cyber/critical-controls/>

Cyber Streetwise

<http://www.cyberstreetwise.com>

Cyber Essentials

<https://www.cyberstreetwise.com/cyberessentials/>

Get Safe Online

<https://www.getsafeonline.org/>



**ANY  
QUESTIONS?**

# CONTACT DETAILS

[gavin.webb@avonandsomerset.pnn.police.uk](mailto:gavin.webb@avonandsomerset.pnn.police.uk)  
[SWRCCU@avonandsomerset.pnn.police.uk](mailto:SWRCCU@avonandsomerset.pnn.police.uk)

07557 083226  
0117 372 2446

DI Gavin Webb  
DS Aled Jones

*Zephyr*  
**RCCU**  
South West  
Regional Cyber Crime Unit

