# Menu of free cyber services

NORTH WEST REGIONAL ORGANISED CRIME UNIT

## Cyber Security Staff Training

We offer a range of training packages to help strengthen your cyber resilience through training your staff and colleagues on the basics of cyber security and how it impacts on an organisation. These can be tailored to your specific needs and include topics such as, cyber crime trends and digital footprints and responding to a cyber incident; using the latest guidance from The National Cyber Security Centre (NCSC).

*Available to all Public Sector organisations, Education Sector (including Universities), Charities Businesses – Senior Leadership Teams (SLT), Board Members, Governance, UK Bodies/Federations, Supply Chain.*

## Cyber Resilience Planning & Exercising

*Do you know what to do if your organisation suffers a cyber attack tomorrow?*

*Does your organisation have a Cyber Incident Response Plan to help you get back to "normal"?*

*Have you ever tested your organisation's cyber resilience?*

We offer different packages to equip Senior Leaders with the knowledge they will need to begin planning their organisation's response to and effective recovery, following a cyber incident.

Learning through interactive scenarios and creating discussions within your teams, we will help you identify what is needed to be included in your organisation.

***Decisions & Disruption Game***

*Designed to explore the decisions organisations make to protect from modern day threats, such as hacking and malware attacks, in addition to physical security and crime prevention.*

***NCSC Exercise in a Box***

*An online tool which helps organisations find out how resilient they are to cyber attacks and practise their response in a safe environment*

FOR MORE INFORMATION & REGISTRATION CLICK HERE

## NCSC Early Warning Service

The NCSC's Early Warning service processes a number of UK-focused threat intelligence feeds from trusted public, commercial and closed sources, which includes several privileged feeds not available elsewhere.

By providing details of the assets your organisation owns, Early Warning will deliver feeds of the following types of threat information:

**Incident Notifications** - Activity that suggests an active compromise of your system.
Example: Your IP address has been involved in a DDOS attack.

**Network Abuse Events** - Indicators that your assets have been associated with malicious activity.
Example: A client on your network is a part of a Botnet.

**Vulnerability Alerts** - Indications of vulnerable services running on your assets.
Example: You have a vulnerable port open.

Early Warning complements your existing threat intelligence products, and should not be used in isolation.

FOR MORE INFORMATION & REGISTRATION CLICK HERE

## Police Cyber Alarm

Helping organisations monitor and report the malicious activity they face from the Internet allows them to understand and monitor malicious cyber activity. It provides both a monitoring and vulnerability scanning service.

Acting as a "CCTV camera" monitoring the traffic seen by the connection to the internet, it will detect and provide regular reports of suspected malicious activity, enabling organisations to minimise their vulnerabilities, protecting personal data, trade secrets and intellectual property.

Members of Police CyberAlarm will become part of the wider UK cyber defence network, sharing collected data with Police for analysis at local, regional and national levels to identify trends, react to emerging threats and identify, pursue and prosecute cyber criminals.

Vulnerability Scanning can be added and used to scan an organisations website and external IP addresses, providing regular reports of all known vulnerabilities

FOR MORE INFORMATION & REGISTRATION CLICK HERE

POLICE CYBERALARM

## Active Cyber Defence (ACD)

The ACD programme seeks to reduce the harm from commodity cyber attacks by providing tools and services, free at the point of use, that protect against a range of cyber security threats.

1. *Protective Domain Name Service (PDNS)* **Eligible sectors**: Public Sector ONLY
2. *Web Check* **Eligible sectors**: Public Sector and Academia (Universities and Further Education Colleges only). Charities (**pilot users only**)
3. *Mail Check* **Eligible sectors**: Public Sector and Academia (Universities and Further Education Colleges only). Charities (**pilot users only**).
4. Host Based Capability (HBC) **Eligible sectors:** Public Sector (Central Government)
5. Logging Made Easy (LME) **Eligible sectors**: Anyone can download and use LME
6. Vulnerability Disclosure **Eligible sectors**: Anyone can report a vulnerability in a UK government online service.
7. Exercise in a Box (EinB) **Eligible sectors**: Anyone can download and use EiaB
8. Suspicious Email Reporting Serice (SERS) **Eligible sector:** Anyone can use SERS
9. The NCSC Takedown Service **Eligible sector:** Public Sector

FOR MORE INFORMATION & REGISTRATION CLICK HERE

## Cyber Sharing Information Partnership (CISP)

CiSP is a joint industry and government initiative set up to exchange cyber threat information in real time, secure, confidential and dynamic environment, increasing situational awareness and reducing the impact on UK business.

FOR MORE INFORMATION & REGISTRATION CLICK HERE

**To book an appointment with the North West Regional Cyber Crime Unit's Cyber Protect Team**

Titan.Cyber.Protect@nwrocu.police.uk

0151 777 7635

NORTH WEST REGIONAL ORGANISED CRIME UNIT