Advising organisations to improve their cyber resilience

Following Russia's further violation of Ukraine's territorial integrity, the **National Cyber Security Centre** (NCSC) has called on organisations in the UK to bolster their online defences.

The NCSC – which is a part of GCHQ – has urged organisations to follow its guidance on **steps to take when the cyber threat is heightened**.

While the NCSC is not aware of any current specific threats to UK organisations in relation to events in and around Ukraine, there has been an historical pattern of cyber attacks on Ukraine with international consequences. The guidance encourages organisations to follow actionable steps that reduce the risk of falling victim to an attack.

You can also check your incident response plan is up to date. See the NCSC's I**ncident Management guidance.**

- Ensure your incident response plan and the communication mechanisms it uses will be available, even if your business systems are not.
- Make sure everyone knows how to report suspected security events and why reporting during a period of heightened threat is so important.
- Confirm that your backups are running correctly. Perform test restorations from your backups to ensure that the restoration process is understood and familiar.
- Check that there is an **offline copy of your backup** - and that it is always recent enough to be useful if an attack results in loss of data or system configuration.

To further support organisations of all sizes and citizens in how they can bolster their cyber security in response to the current situation in and around Ukraine, the following audience-appropriate information is available:

- Critical National Infrastructure, large organisation and public sector - **NCSC alert**
- Small & Medium Enterprises - **Small business guide**
- Microbusinesses, sole traders - **Cyber Action plan**
- Citizens - **www.cyberaware.gov.uk**

For further updates and guidance, please follow:

NCSC: Action Fraud:

Recommended NCSC services available to businesses:

CiSP: Register (free) for the NCSC **Cyber Security Information Sharing Partnership**. This is a secure, online forum to exchange cyber security information in real time, in a confidential and dynamic environment. Membership increases situational awareness through the sharing of threat assessments, advisories, alerts, and vulnerabilities.

Early Warning service: Register (free) for the NCSC **Early Warning** (EW) service. EW is designed to help organisations defend against cyber attacks by providing timely notifications about possible incidents and security issues. The service automatically filters through trusted threat intelligence sources to offer specialised alerts for organisations so they can investigate malicious activity and take the necessary steps to protect themselves.

Board Toolkit: The NCSC **Board Toolkit** covers a range of cyber security topics, starting with an introduction to cyber security specifically written for board members. Other topics include understanding the threat, collaborating with suppliers and partners, and planning a response to a cyber incident. Each topic is filled with straightforward guidance and helpful questions that board members can ask their technical teams.

Exercise-in-a-Box: Register (free) for the 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.

Recommended Police services available to businesses:

Police CyberAlarm: is an award-winning free tool, provided by your local Police Force, to help your business or organisation monitor and report the suspicious cyber activity it faces. The service is made up of two parts: monitoring and vulnerability scanning. It will detect and provide regular reports of suspicious cyber activity, enabling your business or organisation to identify and take steps to minimise your vulnerabilities.

Police CyberAlarm is a monitoring system and does not interfere with normal network operations. More information about Police CyberAlarm can be accessed here: **Police CyberAlarm**

Cyber Resilience Centre (CRC): There is a police-led, not for profit Cyber Resilience Centre in every region in England and Wales (outside of London which is planned for later in 2022) to help businesses better protect themselves against cyber threats. Each CRC offers flexible membership packages to suit the needs of all businesses with the Core Membership being free of charge.

Visit your local centre's website to discover the full range of available cyber security services here: **Regional Centres - National CRC Group**

Reporting a live cyber attack

If you are a business, charity or other organisation which is currently suffering a live cyber attack (in progress), please call Action Fraud on 0300 123 2040 immediately. The service is available 24 hours a day, 7 days a week.

A live attack is one that is ongoing, that is still affecting your system and your ability to work and there is an opportunity for law enforcement to stop the attack and/or secure evidence that will assist an investigation.

Reporting fraud or cybercrime to Action Fraud

You can report fraud or cybercrime to Action Fraud any time of the day or night using their **online reporting tool.** Reporting online is quick and easy. The tool will guide you through simple questions to identify what has happened. You can also report to us by calling **0300 123 2040** Monday to Friday 8am - 8pm.

Report a cyber security Incident to the NCSC

You can report a cyber security Incident to the NCSC here: **Reporting a cyber security incident (ncsc.gov.uk)**

Cyber security incidents reported using this form are monitored 24/7 by a NCSC defence watch officer who will endeavour to reply at the earliest opportunity.