Cyber Security Risk

The National Cyber Security Centre (NCSC), the UK's technical authority on cyber security, have issued guidance for organisations on the steps they need to take to bolster the UK's resilience against the heightened risk of malicious cyber incidents in and around Ukraine.

Many organisations and businesses in the UK have well laid out plans and good cyber security measures in place. However due to the nature of online global networks, attacks that occur overseas could have an impact on UK institutions, services and systems. This is why organisations and businesses are being urged to take action now.

While the NCSC is not aware of any current specific threats to UK organisations in relation to events in and around Ukraine, the guidance encourages organisations to follow actionable steps that reduce the risk of being impacted by cyber attacks, including:

- patching systems
- improving access controls and enabling multi-factor authentication
- implementing an effective incident response plan
- checking that backups and restore mechanisms are working
- ensuring that online defences are working as expected, and
- keeping up to date with the latest threat and mitigation information

Further advice and resources on what action to take when the cyber threat is heightened can be found on the NCSC website.

We would also encourage you to follow the NCSC's social media channels: LinkedIn and Twitter for further alerts and updates.

If you have any questions, please contact enquiries@ncsc.gov.uk.