National Cyber Security Centre
a part of GCHQ

Essential Service Providers
Cyber Security Advice and Support

The National Cyber Security Centre (NCSC) recognises that your organisation is an essential part of the UK's response to the COVID-19 pandemic. As the current situation evolves, attackers could exploit this unprecedented event and the ensuing rapid IT and organisational change that you are likely to be undergoing.

As an Essential Service Provider, the NCSC wants to help you mitigate any increased cyber threat at this critical time. This document highlights the most important preventative measures that you can take to reduce the likelihood of becoming a victim. It also outlines support that the NCSC can provide to your organisation.

Prevention measures

There are several pieces of existing NCSC guidance that are crucial at this point in time. We recommend that your organisation reviews your current approach against this guidance as a matter of priority. However, we encourage you to implement any required changes at a measured pace, taking into account your normal business and risk management processes.

- Mitigating malware and ransomware attacks
- Protecting backups stored in the public cloud
- Mobile device guidance
- Denial of Service guidance
- Home working guidance

In acting on this guidance, please note that:

- The risk of outage or business impact from unplanned changes to IT systems may outweigh the potential security gains at this point in time.
- You should continue with any planned upgrades, patching regimes and security enhancements as normal.

Cyber incident management

All Essential Service Providers are encouraged to report an incident to the NCSC's Incident Management team as a matter of urgency if you experience either of the following:

- Significant loss of data, system availability, or control of systems.
- Unauthorised access to, or malicious software present, on IT systems.

You can report 24/7 via the online reporting form.

To enable us to provide the most effective and timely support in the event of an incident, it would be helpful if you could please reply to your NCSC contact with the following information as soon as possible:

- Contact details for the person or people in charge of cyber security at your organisation (ideally 24/7 contacts if available, to enable us to notify you as soon as possible)
- The name of your incident response company (if you have one on retainer) and a contact at the organisation.

If you do not have an incident response company, as an Essential Service Provider we recommend that you investigate obtaining the services of one. You can find details of the NCSC's Cyber Incident Response scheme on our website, along with a list of certified companies.

Automated notification of cyber security issues

The NCSC can provide reporting to Essential Service Providers of cyber related events to help secure and protect your IT infrastructure. The NCSC processes actionable threat information to establish indicators of malicious activity and compromise as well as identify vulnerable network services. This threat information is gathered from information security groups and initiatives who track and identify malware activity. It can be shared with you to help speed up detection and recovery from malware infection. To do this, we will need you to provide details of your Internet-facing IT infrastructure, including external public-facing IP addresses and registered domain name(s).

A registration form is attached.

Cyber Security Information Sharing Partnership (CiSP)

You can sign up to CiSP which enables the NCSC to exchange cyber threat information with you in real time, in a secure, confidential and dynamic environment. This will assist you in keeping ahead of the emerging threat.

When you apply to join CiSP, you will be asked to provide sponsor details. To enable us to fast track your application, please use the following sponsor details:

Sponsor name: ESP Engagement

Sponsor organisation: NCSC

Sponsor email address: esp.cisp@ncsc.gov.uk