National Cyber Security Centre
a part of GCHQ

Working with the NCSC during a cyber security incident

Who are the NCSC?

Cyber threats to the UK are growing in frequency and sophistication, which is why the government formed the National Cyber Security Centre (NCSC) – the UK's technical authority on cyber security.

We offer unrivalled real-time threat analysis, defence against national cyber attacks, technical advice on cyber security, and response to major cyber incidents to help minimise any harm (including reputational damage) they cause to victims.

We are **not a regulator**. We provide free and confidential advice and guidance on cyber security. Note that the level of support we can offer is prioritised based on overall impact on the UK's national interests. For more information go to www.ncsc.gov.uk.

How can we help with your cyber incident?

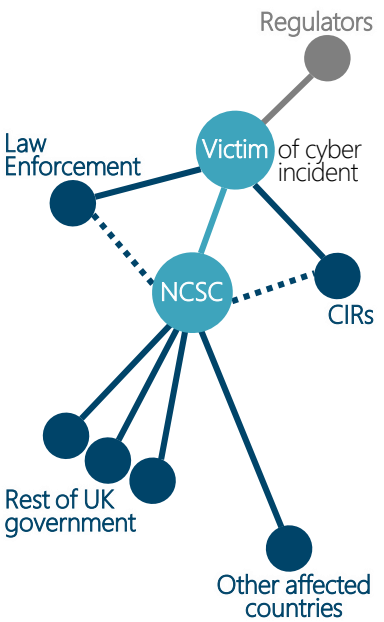
If you have experienced a major cyber incident, we can:

- Provide **technical advice and guidance**; in some circumstances we may deploy incident response to provide direct technical support;
- Use our unique access to information as part of GCHQ to **understand the incident better** – identifying the attacker, their likely motivations, if there are other victims, and if the compromise is likely to spread;
- Coordinate any **cross-government response**, helping you to work with relevant government bodies, and ensuring public communications are aligned.

Who we can work with in support of you:

We encourage reporting to **law enforcement**, who also support, investigate and respond to cyber incidents. A criminal investigation can lead to disruption & prosecution of the perpetrators, helping to prevent future attacks. If the victim agrees, the NCSC will work hand-in-hand with partners in law enforcement, including the NCA's National Cyber Crime Unit, Regional Organised Crime Units (ROCUs) and Action Fraud. The NCA will be involved in the same incident coordination process to ensure consistency of information and action.

Major incidents usually require action from multiple **UK government departments or devolved administrations**. The NCSC manages the flow of information across government, pulling together the latest analysis and agreeing response activities. The NCSC's focus will be on limiting the impact on your business: working with you to manage any security or commercial sensitivities, keeping you sighted on developments, and leading on HMG's media lines related to the cyber incident.



The NCSC is **not a regulator**. We will encourage victims to consider their regulatory obligations (e.g. under GDPR or NIS), but recognise that any regulatory reporting or cooperation must be led by the victim. Note that many regulators will view early engagement with the NCSC as a positive factor when considering regulatory responses.

The NCSC's **CIR (Computer Incident Response)** scheme consists of companies which we have evaluated as expert in responding to cyber incidents. The NCSC is able to work closely with CIRs during incidents, for example sharing sensitive information such as the nature of the compromise or the attacker's methods. Of course, this close working will only be with the victim's permission and ongoing involvement. For more details visit: *www.ncsc.gov.uk/scheme/cyber-incidents*

Where an incident has cross-border implications, we may seek to notify **international partners** whose networks might be impacted by the incident. We will work with you when we do this to manage any security or commercial sensitivities.

What happens to information shared with NCSC?

Any information the NCSC receives from victims of cyber incidents is protected in the same way we protect our own confidential information: held securely, with strictly limited access.

We only share a victim's information with other organisations if we have the victim's permission to do so, or in highly exceptional circumstances if there is an extremely serious public interest reason such as protection of national security. Our statutory powers allow us to disclose information only when necessary for the proper discharge of our own functions *[section 4(2) Intelligence Services Act 1994]* and not for any other purpose (such as any regulatory functions).

As part of an intelligence agency the information we hold is exempt from Freedom of Information requests.

When should I contact the NCSC?

You should ask the NCSC for help if your organisation has experienced a severe cyber incident which poses a risk to your ongoing operation or to your customers or supply chain.

We also appreciate reports of less severe incidents, for information only, to help us further our understanding of key adversaries, revise our guidance, or potentially help to protect other organisations. For more information visit: www.ncsc.gov.uk/incident-management

Note that **you can contact us, 24x7, at:**
www.ncsc.gov.uk/report-an-incident
(Do not use a compromised network to report).

For any other incidents or cyber-related crime, contact Action Fraud at: www.actionfraud.police.uk/report_fraud