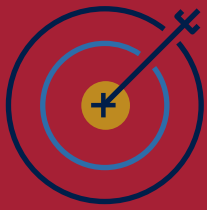
National Cyber Security Centre
a part of GCHQ

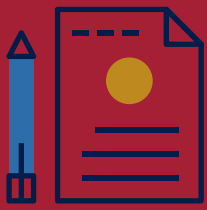
Responding to a cyber incident – a guide for CEOs

Who is this guidance for?



This guidance helps CEOs in public and private sector organisations manage a cyber incident. It sets out aspects to consider at the start of an incident and throughout it.

Why do I need this guidance?



If your organisation is victim of a significant cyber attack, the immediate aftermath will be challenging. You may find there is a lot of information in some areas, and none in others. There will be difficult risk-based decisions to make to protect your operations. Your aim will be to limit the impact on your business, clients and staff in the weeks and months that follow.

Put in place proportionate and effective governance

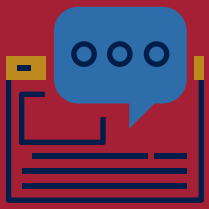
A cyber security incident isn't just a cyber security problem. It's also a business continuity and communications issue, and can be a financial and legal one too.

It may be helpful to appoint a separate SRO (Senior Responsible Officer) or to use a broader governance command structure, bronze, silver and gold model to assign overall responsibility for the incident.

To help your team make effective decisions, you should make sure structures are in place to:

- take account of the **full** impact across the **whole** organisation
- make it easy for those managing the response to regularly come together
- inform and empower senior decision-makers by explaining how technical issues impact them
- allow a robust response to all the demands of an incident (internal and external communications, working with regulators and insurers, providing updates to the board)

Bring in resources for advice and support



Surrounding your teams with reliable external experts who can take an objective view can significantly improve the quality of decision making and help you manage the legal, technical, operational and communications considerations that a serious incident brings. The role of these experts is to provide advice, not to make key decisions.

The NCSC also advises using a cyber incident response (CIR) company to help you manage and recover from the incident. The NCSC assures a number of CIR companies.

If your organisation has cyber insurance in place, you should let your insurer know, as they may have in-house or preferred CIR companies, as well as other services to help you during a cyber incident.

Consider the impact of a data breach

Once a cyber security incident is resolved, there are often still outstanding questions about the risk to data, whether the data is your own, or customer and staff data that you hold. **It is critical that you communicate any risks to data to the data owners, and that you consider the regulatory requirements you may have to report breaches.**

The ICO (Information Commissioner's Office) has guidance on personal data breaches which sets out clearly how to respond to a suspected breach. The ICO is clear that you must report a notifiable breach to them 'without undue delay' and not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

Think about your public messaging

Effective and transparent communications in a crisis won't just reassure your employees, but could also help protect your organisation's reputation externally. Any communications should be factual, clear, and you should be careful not to misrepresent or downplay the incident in a way that creates future difficulties or relationship issues.

You might need to give a different level of detail to different groups – key decision-makers and stakeholders in your organisation, wider staff, your partner organisations or communications to the public. Make sure you know in advance who needs to be brought in to your communications planning.

In a ransomware attack, consider the risks of making a payment

If your organisation is the victim of a ransomware attack, you may find the actor sets tight deadlines for payment. You should read the NCSC's guidance pages on ransomware and payments.

The NCSC and UK law enforcement don't encourage, endorse or condone the payment of ransom demands – but you should be aware that there are risks around making payments to criminals, and that if you do pay, there is no guarantee that you will get access to your data or networks. Research shows that it's also more likely that you will be targeted in future.

Consider team resilience and welfare

During a crisis, staff at all levels of your organisation will probably experience stress and uncertainty, which can be extremely detrimental. You should put their welfare and morale at the top of your response plan. The NCSC has guidance on staff welfare during an incident.

Incidents often start with an intense period of activity, but many incidents also have a 'long tail' with the impact lasting for months. The team will need to make important decisions throughout, but particularly when you are working out how to rebuild and prevent future incidents. It's important to make sure that staff aren't exhausted.

Staff with incident experience are very valuable to an organisation, and putting in place good wellbeing practices may also have the benefit of helping to retain staff in the long term.

Review the lessons learned

Following the incident, make sure there is a debrief with those who helped manage it. You should consider both the things that went well and what you would do differently. This also helps with staff welfare.

You should carry out a review with a genuine intention to learn from the experience and to understand what factors led to the incident in the first place. This should be systemic in nature rather than trying to pin down a single root cause. Your aim here should be to prevent and improve for the future, not to apportion blame.

There will be many factors in play and it's important to understand how they relate to each other to improve your organisational resilience.

Carrying out a general cyber security review should also be a priority to help understand and manage any vulnerabilities in your systems that may lead to further attacks.

The NCSC Cyber Security Toolkit for Boards helps embed cyber resilience and risk management through the whole organisation, including its people, systems, processes and technologies and is a good starting point.

Report it

And finally, you should report significant incidents to the NCSC and UK law enforcement who can provide support. This also enhances understanding of the threat landscape, helping to prevent further incidents and improve security for everyone.

Report your cyber incident using the UK government signposting tool which lets you know which organisations to notify, based on the circumstances of the incident.