When cyber attacks happen: helping organisations recover

A highly disruptive incident can feel overwhelming. New guidance provides a framework for response and recovery.

Some say they felt sick. Others say it was like being punched in the stomach.

However it hits you, finding out that your organisation is the victim of a highly disruptive cyber attack is a real blow.

And as technology evolves and cyber threats continue to grow in scale and sophistication, more organisations are having to prepare for the possibility of serious disruption.

Your first reaction is likely to be an emotional one:

- shock at the news
- anger that your organisation has been targeted
- despair as the full impact of the attack becomes clear
- guilt that the organisation wasn't as well defended as it could have been

All of these feelings – and more – are normal. From day one, victim organisations need to recognise the toll the incident will take on people, work hard to support those dealing with it, and lessen the effects as much as possible.

A framework for recovery

Our new response and recovery guidance will guide you through a highly disruptive cyber incident. It shows that organisations can and do recover from even the most severe attacks and provides a framework to understand what has happened, deal with the impacts, and move forward to full recovery.

The guidance is split into 3 sections, so that you can focus on the key aspects for the challenges you're facing as your recovery proceeds.

The first hours matter

First is how to deal with the initial few hours and days, as you're working out what's happened, what the impact is and trying to coordinate your actions. It emphasises the importance of swift defensive actions, establishing governance and getting control of communications. It also covers the actions to get onto straight away that will help you further down the line and speed up your recovery.

At the NCSC, we see serious cyber incidents all the time so we know the importance of bringing in qualified and experienced help, not just from a technical standpoint but from the reassurance it provides the victim that they're getting the best help available. That's why we always recommend organisations secure the services of an NCSC-assured Cyber Incident Response (CIR) firm.

Building your recovery programme

The second stage is focused on building and implementing your recovery programme. This programme is key to getting your organisation back up and running, to minimum viable operations (MVO). Recovering core business functions quickly isn't just about restoring technology; it's about enabling the organisation to continue delivering services, supporting customers and maintaining confidence in its operations. All your actions must be driven by a business-led view on your most important business functions. Getting these back up and running, sometimes supported by temporary workarounds, brings you to the end of this second stage.

Beyond recovery: rebuilding stronger

The last stage is the longer term rebuild. This is a distinct shift from the recovery stage, and focuses on getting the organisation back to business as usual or – better still – stronger than before. It includes ensuring you address the issues that contributed to the incident occurring in the first place, and taking the opportunity to rebuild in a more secure and resilient way. For many organisations, that includes designing and building systems so that fundamentals – such as patching, configuration and access control – are possible and easier to achieve.

Prepare before you need it: practice and test

Of course, it's best to prepare and practice for these types of incident in advance. Organisations that act early are often better placed to respond effectively, maintain critical operations and recover more quickly. The guidance will help you develop plans and test your response arrangements before an incident occurs.

It's a bit like training for a marathon. Reading about the race, buying the right equipment and writing a training plan are a good start. But it's the actual running – regularly putting in the miles and building endurance – that prepares you for race day.

In the same way, it's vital that organisations don't just document a plan, but actually practice and test their response to disruptive incidents. Testing failover systems, rehearsing shutdown and restart procedures, and rebuilding systems from backups can all provide valuable real world lessons. While tabletop exercises have their place, realistic response exercises can reveal issues that plans alone cannot. This helps organisations to:

- learn lessons they wouldn't otherwise learn
- more importantly, build the 'muscle memory' needed to respond effectively under pressure

Now it's up to you to use the guidance to do just that.

Ralph B

Chief Technology Officer Economy & Society, NCSC

WRITTEN BY

Ralph B

Chief Technology Officer, Economy & Society, NCSC

PUBLISHED

28 July 2026

WRITTEN FOR

Cyber security professionals Large organisations Self employed & sole traders Small & medium sized organisations

PART OF BLOG

NCSC publications