THE RECOVERY GAP

Why having a continuity plan isn't the same as being able to recover from cyber attacks and the disruptions caused by them.

Research and analysis writer for B2B technology, specialising in cyber security

This is a demonstration report with illustrative case studies.

S & S Edlington Ltd.

August 2026

INTRODUCTION

Most medium-sized firms have an incident response plan. But fewer companies now have a business continuity plan that covers cyber security, down from 53% (2025) to 44% (2026).[1]

Being subject to a cyber attack is one thing; not being able to get the business running again as soon as possible is another entirely. And in many ways, far more of a threat than the attack itself.

As cyber threats enter a new era and new tools make it easier for criminals to create more sophisticated and effective attack strategies, companies are understandably focused on how to protect their systems.

Additionally, regulators, suppliers, customers, stakeholders and investors expect more from a company's security posture.

A company needs to show it's protecting the business and what measures it has in place to recover quickly when the worst happens.

#1 THE PLAN-VERSUS-PRACTICE GAP

Having a continuity plan is good, but if all aspects of it haven't been tested, the company won't know how resilient it is to disruptions. It's an assumption, rather than reality.

One untested area of a plan can turn an incident that a company can contain into one that causes problems for days, weeks or even months.

Listed below are the areas that can be missed during routine testing.

This can happen when one team assumes another team is responsible, and can leave critical gaps in a continuity plan.

Backup integrity. Backups, and backup devices such as tape drives, need to be isolated, protected and regularly tested.

Identity and Authentication. If single sign-on (SSO), multi-factor authentication (MFA) or passwordless authentication are compromised, staff will need alternative secure means of accessing systems.

Supply chain and third-party dependencies. Companies need to look at these in broad terms. A supplier might only be used once a year, but the service they provide is part of a critical chain within the company.

Legacy systems. These can be wide-ranging, including: VOIP (Voice Over Internet Protocol) desk phones, old webcams built into laptops, NAS (Network Attached Storage) backup boxes, and other devices that are no longer supported by their supplier.

As these may only connect to the network occasionally, they still need to be included in a continuity plan.

When these have been checked, testing is the next step. However, unless this is done correctly, a company could still be at risk of disruption.

#1 THE PLAN-VERSUS-PRACTICE GAP CONTINUED

Testing only proves a company's resilience when it goes beyond being a document and is tried out under real-life conditions. Below are the main best practices for doing these types of tests.

Use different types of tests. Companies need to use a mix of exercises and also test across their organisation so each department understands their role when an attack happens.

These exercises can include table-top, live simulations, incident response walkthroughs and communications scenarios.

Use realistic scenarios. Plan for data loss, ransomware attacks, infrastructure failures, and sabotage (such as undersea cables) that can lead to cyber attacks, and use official toolkits such as the National Cyber Security Centre's Exercise in a Box.

Third-parties. Include any third parties the company depends on, and test how the company can function if it were to lose access.

Communications. Decide what alternatives will be used instead of the usual communication methods.

Team members and other staff. An attack is mentally and physically stressful for a company's employees. Testing how they will cope means a company can put in place measures to support them.

Illustrative case study

A small manufacturing firm relies on two legacy systems that hold technical data they use several times a year. The company believed that as neither system is connected to the main network, they were safe and didn’t need to be included in their continuity plan.

However, a security audit showed the legacy systems could be compromised if an infected memory stick was used to transfer data from them. Though the systems were low-use and unconnected, they were still a 'hidden' security risk for the company.

#2 THE RECOVERY TIME REALITY

The real cost isn't the disruption or attack; it's the time and effort it takes to get back to normal.

A company will lose revenue; customer and supplier trust can be affected; customers may go elsewhere because they can't access the services they want; and breaches will need to be reported to the relevant regulator.

Additionally, devices or systems may need to be replaced, and staff will need time to recover from the crisis.

In fact, research from Fastly [2] shows that IT decision makers underestimate how long it will take to recover from a cyber incident. The IT decision makers estimated it would take 5.85 months. The actual time was 7.34 months.

Recovery times can be affected by various issues which a company can cover in their continuity plan.

Poor documentation. Staff need to know where incident documents are stored. The documents need to be easy to read for non-technical staff, clear about roles and what happens in different situations, and explain who to contact, with emergency contact numbers.

Slow data restore times. Restoring data can take a lot longer than a backup. Each type of restore needs to be checked and timed; this way the company has an idea of how long each type will take. And this can then be added to the continuity plan.

Third-party dependencies. Many companies rely on others to supply them with certain services. It's worth checking contracts to see how long restore times are and what happens if a restore is needed out of office hours.

Incomplete removal of the threat. Removing threats can be time-consuming and involve rebuilding systems infrastructure, dealing with system interdependencies, and compromised backups.

Once a company has this information and data, they can find ways to effectively reduce recovery and downtime as much as possible.

#2 THE RECOVERY TIME REALITY CONTINUED

How long it takes for a company to recover from an attack will depend on the size and scale of it. However, companies can prepare, giving them a good idea of the time it will take to get systems operational again.

Include defined RTOs and RPOs in the continuity plan. RTO (Recovery Time Objective) is the maximum amount of time a company's systems can be down following a disruption before it causes considerable harm to the business.

It's also a metric for how quickly those systems or processes need to be restored so the business can resume operations.

RPO (Recovery Point Objective) is the company's threshold for acceptable data loss. When data is recovered, some data may be lost in the process.

Using an RPO, a company can work out how far back in time they need to go to get their business back to normal operations. For example, an RPO of 2 hours means the company could lose 120 minutes of information and data, as backups are made every 2 hours.

Map critical systems. These are systems or processes the company doesn't have direct control over. Knowing how long it would take to restore this is another critical data point for a continuity plan.

Illustrative case study

A mid-size firm had a continuity plan but had never tested restoring its backups in a real-life scenario.

Their plan suggested it would take two working days to restore their data and information.

When ransomware hit, the restore took nine working days, leaving the company unable to run properly during that time.

The company's plan was sound; however, as it had never been tested, the timings were assumptions based on old restore times.

#3 THE DEPENDENCY BLINDSPOT

A company’s continuity plan can have a gap. If some of a company’s operations are run by a third party, then when a disruption happens, a company’s recovery time now depends on its provider’s continuity plan.

These third parties can be a cloud host, a managed service provider, a business partner or a critical supplier whose control systems a company can’t recover on its own. And how much they can affect a company can easily be missed in a continuity plan.

Potential issues can include:

Data breach or data loss. If a supplier holds a company's data and it's attacked, the company's data and information could be compromised or inaccessible.

Outage or disruption. If a company's MSP (Managed Service Provider) suffers a disruption, then a company may not have access to what it needs for daily operations.

Unable to access cloud services. A failure in one region of a company’s cloud host causes access problems.

Software supply chain attack. Infected or compromised third-party software, patches, or other updates are installed onto a company's system.

Credential theft. A company's systems are attacked using credentials that have been stolen from a supplier or third party.

Data at rest and in motion. If a company has data stored with a third party and it isn't encrypted, it could be compromised either 'at rest', where it is stored, or 'in motion' when it is transferred between the supplier and the company's systems.

Including third-party business relationships in a continuity plan means taking a broad look at the services and data that are being used and stored with them.

After a thorough audit, a company can now include their suppliers in their continuity plan.

#3 THE DEPENDENCY BLINDSPOT CONTINUED

As the systems and services provided by a third party are largely out of the company's direct control, risk management and ensuring a company is as protected as possible is an important part of a continuity plan.

Ask suppliers for their RTOs and RPOs. A company can ask for specific targets for these, such as mission critical, business sustaining and administrative.

Mission critical can be defined as real-time data and infrastructure, depending on what a company decides is mission critical for their organisation. Business sustaining is for non-urgent data processing and secondary tools like software. Administrative covers archive access and other, non-essential background services.

Contracts and Service Level Agreements. The RTO, RPO, and other information, depending on the company's requirements, need to be documented in the contract with the supplier so each party knows what will happen and when.

Third-party continuity testing. A company needs to include their third-party suppliers and partners in their audits and testing. These can include similar tests a company uses for its own continuity testing.

Ask for evidence. Ask suppliers if they have certifications such as Cyber Essentials Plus, ISO/IEC 27001 (Information Security Management System) and ISO 22301 (Business Continuity Management System).

Illustrative case study

A consultancy was using a cloud service to allow their staff to access the company’s information and data when they visited clients. Their continuity plan included an assurance from the cloud service provider that they could always access their information.

A fire at an electricity substation caused the cloud service provider’s systems to go down, leaving the consultancy’s staff unable to access information and data for several days.

Going forward, the consultancy realised that assurance is not a guarantee and now tests what 'always available' means in practice.

CONCLUSION

Having a continuity plan is one thing; however, unless it’s tested, timed, and staff know what to do, it will not work when it's most needed.

With the structures and systems in place, when a company’s operations are disrupted, everyone will know what to do, when to do it and how long it will take before the business is up and running again.

Knowing that a company is prepared and ready for either an attack or other disruption is reassuring for the company and everyone else involved with it, from customers to investors.

References:

(1) Department for Science, Innovation and Technology’s Cyber Security Breaches Survey 2025-2026 – Section 3.8 Cyber security policies and other documentation.

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-20252026/cyber-security-breaches-survey-20252026

(2) Fastly. Cybersecurity at the Crossroads survey of 1800 IT decision makers worldwide, this report focused on Europe, carried out by Sapio. Recovery Time - Preventive measures top the list of recovery tactics - Figure 1.

https://www.fastly.com/resources/industry-report/cybersecurity-at-the-crossroads-europe-2025

ABOUT THE AUTHOR

Sara Edlington was a B2B technology journalist for twenty years. Her work has been published in the UK, Europe and the USA.

She is the author of fourteen non-fiction books and has appeared on BBC television and radio.

Now, she is a B2B technology research and analysis writer specialising in cyber security.

Contact:

Email: sara@sandsedlington.com

Web: www.sandsedlington.com

LinkedIn: https://www.linkedin.com/in/saraedlington

S and S Edlington Ltd is a registered company in the UK.

Registration number: 14303612