triangle

Data recovery for the new post-attack reality

Ensure business continuity and survival with cyber recovery

Content

INTRODUCTION

Turn adversity into opportunity

In today's digital landscape, cyber attacks are not a matter of if, but when. Cyber crime is on the rise all around the globe. Attacks on businesses aren't only becoming more frequent, they're also increasingly sophisticated - and the damage they inflict is more severe than ever. Entire business environments are compromised. Essential systems are unavailable. Data is exfiltrated and encrypted. Revenue, reputation and livelihoods are at risk.

Preventing these attacks is no longer a viable strategy. Businesses must accept that it's only a matter of time before a catastrophic scenario strikes their own digital infrastructure.

Business survival depends on your ability to recover with full data integrity. Recovery, when possible, requires significant compromise. It's time for organisations to enhance their cyber strategy to be future-ready, post-attack recovery in addition to their pre-attack resiliency.

In this guide, we'll explore why demonstrable cyber recovery is essential for business survival and the key principles that ensure your organisation can bounce back, no matter the threat.

01

What is cyber recovery?

Disaster recovery is no substitute for cyber recovery

Traditional cybersecurity focuses on protecting the perimeter of an organisation's network and safeguarding core applications within your environment. Essentially, it focuses on keeping bad actors out of your infrastructure.

Cyber recovery comes into play when those cybersecurity measures fail to prevent a system breach. It refers to an organisation's ability to recover critical services and workloads following a cyber breach or cyber attack.

For that reason, cyber recovery often gets contrasted or compared to disaster recovery (DR), particularly since they each serve the high-level goal of recovering core business services following an event. But disaster recovery solutions and services suffer from critical deficiencies in effectively recovering from a cyber attack in different ways. Some of them are:

1 Traditional DR is tightly **coupled to production environments**

2 DR security layers **are vulnerable to cyber attacks**

3 DR solutions **are not sufficient for CR compliance**

Traditional DR environments are tightly coupled to production

High-speed network links between your two environments allow for data to be continuously synchronised. In the event of a cyber attack, however, this means your DR environment represents a valid attack surface. Any data corruption that occurs within your primary site will eventually permeate into your disaster recovery site.

DR security layers cannot guarantee protection during a cyber breach

Multi-factor and two-factor authentication can improve the security of your disaster recovery and backup environments, but they can't guarantee that these systems won't be impacted. The same is true for immutable storage concepts: since they are accessible across your production estate, they are vulnerable to compromise.

DR solutions aren't sufficient to meet cyber recovery compliance requirements

New legislation and directives in Europe have been established to accelerate maturity within the cyber recovery space. The NIS 2 Directive and the Digital Operational Resilience Act (DORA) have been implemented to enforce compliance across the financial industry, but all organisations across every industry would be well-served by establishing a cyber security position that can help them recover critical business services in the event of a cyber breach.

Remember

A cyber breach is far more likely to occur than a disaster scenario. For this reason alone, organisations should prioritise a recovery framework that can help them ensure business continuity and survival from the most imminent threat to their operations.

02

The 6 key design principles of cyber recovery

6 key design principles of cyber recovery

From a technology perspective, there are a number of key design principles that must be adhered to when establishing a cyber recovery position. Here are the six principles we view as a requirement:

PRINCIPLE 1

Full isolation for your organisation’s target data

The most important design principle is that all target data pulled out of an organisation’s production environment must be fully isolated from your organisation. Unlike traditional backup storage, which can be accessed through your network, full isolation requires physical and logical separation to preserve data integrity in the event of a cyber breach.

PRINCIPLE 2

Secure storage in a cyber vault

A cyber vault is an essential solution for any cyber recovery position, providing a secure, isolated location that is inaccessible from within the organisation. A cyber vault should be invisible from within your organisation’s network and located away from all attack surfaces, ensuring data protection even from the most sophisticated cyber attacks.

PRINCIPLE 3

A strong data forensics or analytics engine

Once the data is secured in this isolated location, data forensics or analytics tools must be available to verify that the data within your cyber vault is healthy. This analysis can serve as an early warning system to your organisation if unhealthy data is identified, which could indicate that a cyber attack is currently underway within your production environment.

The insights from this data can also aid forensics teams as they investigate the possible cause of the breach, as well as the extent of system compromise.

PRINCIPLE 4

Infrastructure to support workload recovery

In addition to isolated storage in a cyber vault, an effective cyber recovery position also requires isolated infrastructure that can be used as a staging area or "clean room" to support continuous recovery testing and live recovery efforts.

Clean room technology provides a safe, controlled space where recovery teams can evaluate data and applications to confirm they are 'clean' before they're restored to your production environment.

PRINCIPLE 5

Continuous recovery testing

Recovery testing allows an organisation to verify its ability to effectively recover workloads with full data integrity in the event of a cyber breach. Certain regulations, including DORA, even require organisations to perform regular recovery testing—and to provide proof of successful recovery testing in the past.

Organisations can also use recovery testing to accurately estimate the amount of time required to recover certain workloads after a cyber attack.

PRINCIPLE 6

Protected copies of all data, not only mission-critical workloads

When recovery begins following a cyber breach, Tier 1 data is the highest priority for your recovery efforts as you work to restore a minimum viable company. However, to recover your entire business after a cyber breach, you need to ensure that you securely store all copies of your business data in an isolated, offline location.

After Tier 1 workloads have been restored, your business can move on to Tier 2 and Tier 3 workloads. While these are expected to take longer to fully recover, they are important to restoring the full range of your business services beyond your mission-critical workloads.

03

What happens when a cyber breach occurs?

Responding to a breach

No organisation wants to be put in the situation of responding to an ongoing cyber breach. Even worse, fast decisions need to be made with only a limited amount of information about the attack. While data forensics teams execute the necessary exercises to understand what has happened and how it has happened, other cybersecurity and recovery processes must leap into action to mitigate the organisation's risk, protect your data, and support a fast, full recovery. A lot of these first steps depend on the testing, scenario-planning, and other steps you've taken to prepare for this event. Here's a high-level overview of what to expect:

1

First, consider whether you need to take your network offline, including your full storage fabrics.

This will impact most or all of your core business services, but it may be necessary based on the estimated extent of the breach. If you take this action, you will inevitably stand up your major response teams.

2

Lean on your rigorous testing cycles to coordinate activities across teams

Recovery exercise is recommended on a quarterly, if not monthly basis, to ensure that all stakeholders understand their roles and responsibilities in recovering your workloads. Rigorous testing instills confidence throughout the organisation and provides the ability for your teams to come together to successfully recover from the breach.

3

Communicate clearly across all teams and roles

Given the many unknowns involved in a cyber attack, clear communication is key to an effective response and recovery. Recovery operations teams and other parties will need to be given specific information and direction to guide their efforts on which services to disable, when to start recovery processes, and which workloads to prioritise first.

4

Use the information uncovered by data forensics experts to guide your response

As forensics teams investigate the breach, they will be able to direct recovery processes in terms of which workloads were affected and how far back in time recovery efforts must go. Your organisation's understanding of the breach will evolve quickly through this investigation, and an agile recovery will be key to your overall success.

04

Day-to-day operations for effective cyber recovery

Requirements for maintaining your recovery position

Once a cyber recovery infrastructure is implemented, ongoing testing, support, and management are required to ensure that your recovery position is always set up for optimal performance when a cyber attack strikes. We encourage every organisation to establish the following protocols for continued confidence in your cyber recovery capabilities:

Separate the management of your production estate from the management of your cyber vault

The individuals who manage your production estate should never be the same individuals tasked with managing your isolated data. If a user's credentials become compromised, those credentials could be used to access the vaulted infrastructure, compromising the data you are dependent upon for any recovery effort.

Test cyber vault solutions to ensure they remain invisible to your organisation's network

Penetration tests are advised periodically to ensure continuous isolation of the vault. This is important even when the vault infrastructure is managed by a third party. If a test discovers that the vault is visible through your network, this means the isolation has broken down, leaving all copies of your organisation's data exposed in a cyber breach. If detected, your recovery experts and vault management team must work quickly to eliminate this visibility as quickly as possible.

Requirements for maintaining your recovery position

Be ready to provide evidence of successful recovery testing at any given moment

Even when this proof is not required as part of compliance law, every organisation benefits from having proof of consistent, successful recovery testing, which offers the practice and confidence your organisation needs to effectively respond to a cyber breach. Recovery testing also lets you evaluate the robustness of your runbooks and, if necessary, revise these protocols to improve future recovery efforts.

Accommodate new platforms and systems within your cyber vault

As your production estate evolves, new production applications will need their own cyber recovery position within your cyber vault. Runbooks will also need to be modified to support the recovery of these new applications or upgraded systems.

05

A proactive solution to future business adversity

Triangle cyber recovery solutions and services

Prevention alone is no longer a feasible tactic for addressing the threat of cyber crime. That's why Triangle's cyber recovery solutions & services provide provides true last-line data protection by physically isolating and safeguarding immutable copies of your critical data away from attack surfaces - enabling a safe, controlled recovery process with full data integrity.

Traditional disaster recovery and cybersecurity won't help your business recover from a cyber attack on your digital infrastructure. It's time to invest in data recovery that can help ensure business continuity and survival in any post-attack scenario.

Remember, it's no longer IF you'll come under cyber attack, it's WHEN. Talk to our cyber recovery experts today to discover how Triangle can secure your critical data and your organisation's future.

info@triangle.ie

+353 1 657 9700

www.triangle.ie

triangle