SYNAPSE 360

4 Keys to Navigating the Cyber Recovery Journey

There has been an exponential increase in the number of newsworthy cyber attacks over the last few years. The most common primary goal? Destroying data. Some attacks simply erase data while others encrypt it and hold it for ransom.

Many data protection and cyber security strategies have not evolved quickly enough to effectively recover from these types of emerging attacks.

Here, Synapse360 explores how developing a cyber recovery strategy can help quickly recover your critical systems and applications.

Claim your free health check

0330 660 0001 hello@synapse360.com synapse360.com

4 Keys for Cyber Recovery

1 Understanding you are the target

Security threats can come from all directions, both internal and external.

They can be malicious or accidental. Un-patched infrastructure firmware, out of date applications, and sabotage from insiders are just a few types of attacks.

When an event happens, the response team must be able to know, quickly and easily, what are the upstream and downstream effects of the disruption. Exactly what systems, offic-es, suppliers and distributors are affected by the event? There needs to be a dynamically created checklist that walks the team through whatever steps need to be taken to respond.

2 Security is built from the ground up

Let's face it, there is no silver bullet for countering security threats.

From improving advanced threat intelligence capabilities and verifying components in the supply chain to improving disaster recovery policies and isolating/ air-gapping resources within a network, businesses are deploying a wide range of approaches to help secure their assets.

IT professionals are now driving towards a stronger, more resilient security posture through a diverse range of initiatives and measures.

3 Every security journey needs frameworks

Over 30% of organisations say they don't use any security framework today, with over 20% indicating they don't plan to within the coming three years. This must change.

No two companies are alike, so you need a tailored strategy that supports your unique requirements.

Simply having secure hardware and software (or thinking that you do) does not replace the requirement for policies and procedures.

Hardware alone isn't security, having the right policies and procedures in places is critically important.

4 Use Cyber Recovery to compliment DR

In a Cyber Recovery event, you might not know what happened, when it started, or what exact-ly was lost. The goal is still to restore normal operations as soon as possible.

A cyber recovery vault needs to be isolated from the network and physically secure. Any system that is connected to the network is potentially vulnerable to a cyber-attack.

Creating an 'air-gap' from the primary network is an effective measure in keeping critical data safe. The vault also needs to be physically secured, and access should be restricted from users without proper clearance.

Claim your free health check

0330 660 0001 hello@synapse360.com synapse360.com