the I.T. insider

Your 3 Step Plan to Achieving Data Resilience

For many businesses ensuring data resilience can seem unobtainable, especially if you're struggling with a combination of on-premises storage from multiple vendors or have been steadily acquiring storage on an ad hoc basis. Team this with the growing popularity of cloud storage and the idea of securing and unifying all of this seemingly disparate data suddenly seems far too complicated and out of reach.

If this sounds familiar and your business is thinking about incorporating data resilience into your business continuity plan, here are some simple steps you can take to get you started on the path to future-proofing your business from data-destructive events.

Step 1 Build an effective data resiliency plan

The first thing you need to do is to determine which data needs to be made resilient. This is the data you use on a daily basis which is critical to your business and if anything happened to it, could potentially stop your business from operating and would be difficult, if not impossible, to recover from.

Taking the time to understand how your data is stored and flows across your network makes it easier to pinpoint vulnerabilities and weak spots which are at greater risk of data breaches, data leaks, and cyberattacks. Once you have this information, you can use it to inform your decisions on the next steps you need to take and the security tools and solutions you need to put in place, to help make your IT infrastructure data resilient; helping you mitigate and quickly recover from any disruptive event or catastrophic failure that could threaten your data and negatively impact your business either financially or reputationally.

Step 2 Modernise storage infrastructure

The simplest and most cost-effective way to achieve data resilience is by modernising your existing storage infrastructure. IBM has a wide range of enterprise-class, software-defined storage that can help you make the most of the assets you already have and upgrade your traditional data storage solutions that are no longer fit for purpose.

Both IBM FlashSystem and IBM SAN Volume Controller use IBM Spectrum Virtualise technology to insulate applications and protect them from any attacks on your physical storage. They not only add greater flexibility to your new and existing storage, they also lower cost and allow applications to run without disruption. Plus, they also give an extra layer of protection by creating immutable copies of your data to protect against ransomware and other cyberthreats. So, if you are attacked, you have the ability to quickly restore and recover these copies and continue your business as usual.

Choosing the right set of data resiliency techniques and technologies is crucial. IBM Storage has combined the modern data resiliency capabilities of IBM FlashSystem and IBM Spectrum® Protect Plus for end-to-end data protection. These easy to use, simple to deploy, cloud-ready solutions provide disaster recovery, replication, retention, and data reuse for VMs, databases, applications, file systems, SaaS workloads, and containers on-premises or in multi-cloud environments.
Once you have everything in place to protect your most valuable asset, you can then move on to the next stage of your data resilience journey.

Step 3 Grow your business

By having a well-thought-out data resilience plan, modernising your storage, and implementing these tried and tested strategies, you should soon start to see a big reduction in the number and severity of cyberthreat incidents, and start benefiting from:

- High availability and secure access to essential data and applications
- Secure and flexible architecture that can withstand any data threat
- Less time spent on troubleshooting and more time spent on innovating
- Increased customer loyalty and a reputation for reliability

Data resilience forms just one part of your wider cyber resilience strategy and business resilience management (BRM), but when you're trying to safeguard everything from data, employees, finances, and brand reputation, it's essential that you seek expert advice and get it right first time.

If you need help evaluating the current state of your data protection, take this free cyber resiliency assessment to identify any gaps, strengths, and weaknesses and get expert recommendations on how you can build an effective data and cyber resiliency plan going forward.