Jonathan Smith, Sword's Cyber Resiliance Technical Lead who has been in the industry for 11+ years. His role at Sword Ping involves working with our customers to help them design network and security to secure and connect their data.

Jonathan Smith

KEEPING BACKUP AND RECOVERY SIMPLE

In today's fast paced world, with changing technologies, we know organisations are faced with the challenge of finding the balance between simplifying technology and designing technology solutions.

Amongst other hurdles faced in an already diverse landscape, it's important for us to keep evolving our environment so we can make the most of secure digital solutions which in turn guides data driven decisions.

With the constant threat and risks to organisations, there must be a constant focus on security practices, threat playbooks and immutable backups & recovery.

Keeping backup and recovery Simple

Backup and recovery are increasingly talked about in multiple different areas of information technology, business, resiliency, cyber security and risk management. Due to this, what used to be a conversation around backing up on-premise infrastructure is now filled with multiple acronyms and terminology which has expanded with the increase in cloud adoption.

At Sword, we have regular conversations with organisations on keeping backup and recovery simple and ensuring that commonly adopted architectures are utilised and are in line with relevant industry frameworks.

So what is the end goal of backup and recovery?

In its simplest form, backup and recovery is about having the correct technical solution and robust processes that can be utilised as part of recovery playbooks to ensure that an organisation can access their data when they need it most and this can span from simple emails to critical data and infrastructure.

Where does the complexity come from?

Complexity can come from things as simple as the amount of acronyms utilised or the solution sprawl that can be seen in older architectures. For example, a single conversation that touches on multiple acronyms like BIA, RPO, RTO, MPTOD, SLA, and BDR can make a critical solution a headache for some departments that not only look after backup and recovery but also the wider technology, security and risk management estate.

What can be done?

When we look to ensure our non-critical and critical data is available to us all we need is a solution that makes it simple to consume, simple to use and simple to secure.

At a minimum, we want our data to be backed up with at least three copies of our data, in two different locations and at least one copy at an off-site location. Then we look to make sure that when this data is backed up, it can no longer be changed ensuring that we have data integrity. Modern-day backup solutions will then split the data into smaller groups at variable lengths to make the most of the storage space available. By utilising modern backup and recovery solutions that have been built with immutability, ransomware recovery and cyber secuirty at the forefront of the technology rather than as an afterthought gives organisations the confidence that their data is secure and accessible when it's needed most.

With cyber security recovery playbooks and incident response, we also want a solution that makes it simple to practice recovery and ensure that we are able to recover within a time that meets business requirements and goals whilst also providing insights into what could be contained within the backup. Does the backup contain a threat to the organisation, has the data been changed but also what information is contained in the data and does it contain personal information?

Final Thoughts

From experiencing incidents that require recovery first-hand, our team of experts always ensure that a solution is in place to provide our customers with the confidence that their data will be kept securely and available at all times. We work with customers to provide an array of security solutions to ensure organisations can continue achieving business outcomes without the burden of potential cyber threats and the damage that will inevitability be caused by these threats.

Having that knowledge and insight into backups allows us to understand what this environment looks like on a regular basis and ensures that when we are asked "How quickly can we bring this back online?" or "How quickly can we recover?" we can be confident that we don't need to rebuild to gain access or have specialist teams provide access to our customer's data.

> **Utilise modern backup and recovery solutions that have been built with immutability, ransomeware recovery and cyber security at the fore front of the technology rather than an afterthought.**