SPONSORED BY

SWORD
UPGRADE YOUR BUSINESS

www.sword-group.com

Jonathan Smith is a Cyber Resilience Technical Lead who has been in the industry for 11+ years. His role at Sword Ping Network Solutions involves working with our customers to help them design network and security solutions to secure and connect with their data.

Craig Neilson is a Sales Lead for Sword. Craig joined Sword 5 years ago and as Sales Lead is responsible for managing relationships with customers to align their requirements with Sword Ping's offerings.


Jonathan Smith


Craig Neilson

Being cyber resilient to protect your data

Changing landscape

The reality for our industry is that it is no longer if you have a security breach but when. With an ever-changing threat landscape, it is more important than ever before to protect your data and have suitable plans in place to recover efficiently.

With the rapid pace of change in technologies and growing challenges, many organisations are striving to find the balance between simplifying technology and designing technology solutions. As an industry continuing to face different pressures in an already complex and diverse landscape, we must continue to evolve our environment to maximise the benefits of secure digital and data-driven solutions.

The importance of cyber resilience

The National Institute of Standards and Technology (NIST) specifies the definition of Cyber Resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources." Due to the breadth of diverse data sources, high data velocity and greater data veracity, we, as industry must stay on top of utilising cyber resources and solutions to be prepared for the increasing potential of cyber-attacks.

The reality for our industry is that it is no longer if you have a security breach but when

Driving Cyber Resilience

At Sword we utilise recognised cyber security frameworks and fit-for-purpose security solutions to assist our customers in their cyber resilience planning such as cyber risk awareness and planning, attack surface awareness, lifecycle management and cloud security.

Without appropriate cyber-resilient solutions and recovery plans organisations will face extended downtime at increasingly high costs.

Organisations today must look at the type of data they hold, whether its internal business, customer data or business critical data. Data today provides significant opportunities to run your business but also exposes organisations to many risks should that data be compromised or breached. What loss would you experience from downtime or GDPR implications? What reputational damage may impact ongoing or future business? These implications are only touching the surface of what needs to be considered on a continuous basis.

Without cyber resilient solutions and recovery plans organisations will face extended downtime and increasingly high costs

Mitigating risks to data

As part of mitigating risk it is advised to start with understanding and identifying risks to your organisation. Going through a risk assessment, treatment and prioritisation plan allows organisation leaders to make decisions based on the probability and impact they may have.

Understanding your attack surface and how many access points to your business exist, allows for the beginnings of a cyber resilience plan to be created. It has long been the focus for many organisations to concentrate on virtual data perimeter security utilising firewalls to create boundaries between data and external threats.

With the continual threat and risks to organisations, there must be a constant focus on security practices, threat playbooks and Immutable backups & recovery. Additionally, it is vital that organisations ensure employees are up to date with the latest end-user security training available to them.

The future of cyber resilience

Over the past three years, the energy industry has been rapidly progressing with digital transformations whilst continuing the road to net zero and maximising operational efficiency. With this transformation additional challenges arise with digital adoption and ensuring staff are up to date with training. Sword 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.

Being cyber resilient to be data driven

If we, as an industry, are to achieve data driven outcomes, we need to ensure that data is placed at the heart of our operational and project thinking. The only way we do this is by ensuring our data sits in a reliable and secure environment and is protected with sustainable security plans to maintain a high level of cyber resilience.

Event

Join us on the
4th of May
for our event: -

'Cyber resilience in a multi-cloud world'

The event will be held in **The Chester Hotel in Aberdeen**, where we will be joined by our partners Cisco and Cohesity.

Please contact **craig.neilson@swordgroup. com** to **register for free.**

About Sword **As the North Sea's largest provider of data and digital services, Sword focuses on solving the industry's most critical business technology challenges by enabling our clients to capture, manage and utilise data to make informed decisions. This is supported by people engagement and technology adoption, together with modern ways of working to give confidence that the right discission is made every time.**

For more information, visit www.sword-group.com

SWORD
UPGRADE YOUR BUSINESS