MEETING THE CHALLENGE

Managed Service Providers play a crucial role in the smooth running of the UK's critical national infrastructure

Martin Riley *puts the NIS2 Directive under the microscope to reveal what it means for Managed Service Providers*

The EU's Networks & Information Systems Directive and Regulations (NIS) aims to improve the cyber security and resilience of critical systems across Europe with the Directive enacted in UK law as the NIS Regulations. First introduced in 2018, the Directive and supporting UK NIS Regulation has no doubt driven significant improvements in the cyber security of our critical infrastructure. Indeed, 76 percent of cyber leaders surveyed in Bridewell's latest research agree that the process has improved their cyber security posture.

However, like most legislation there is always room for further development. While previously only applicable to Operators of Essential Services (OES), the proposed updates to the NIS Directive currently making its way through European parliament, (otherwise known as NIS2) expands the scope to include new sectors based on their criticality for society and the economy. So, for new sectors like Managed Service Providers (MSPs) what could the changes mean?

The NIS Directive has been fundamental in improving cyber resilience, enhancing governance processes, and the identification and management of cyber risk and maturing cyber defence capabilities. But application of the Directive has been particularly inconsistent across Member States of the EU due to uncertainties around its scope. The updated legislation seeks to address this shortcoming by defining a new scope of application supported by more prescriptive requirements, with the UK set to follow suit.

The UK government recently launched a consultation on its proposal to reform the existing UK legislation with the proposed updates including: expansion of the scope of 'digital services' to include 'managed services,' as well as other companies that current entities in scope are critically dependent on; application of a two-tier supervisory regime for all digital service providers: a new proactive supervision tier for the most critical providers, alongside the existing reactive supervision tier for everyone else; creation of new delegated powers to enable the government to update the regulatory framework and scope; strengthening of existing incident reporting duties to include other significant incidents; and extension of the existing cost recovery provisions to allow regulators to recover the entirety of reasonable implementation costs from the companies that they regulate.

The criticality of the new updates is explained by the fact that new sectors like public administration and manufacturers of certain critical products, such as medical devices, will now be included. However, question marks remain around how legislative alterations will translate into practical implementations across each industry, especially with the contrasting maturity levels across different sectors. Regulation is certainly a driver for cyber security improvement, but we must view this development within a much larger context.

MSPs play a crucial role in the smooth running of the UK's critical national infrastructure. They deliver complex activities that require high levels of access – but often without the security architecture, design, governance and operational capability needed to ensure data is kept safe. This has long been a risk that is either misunderstood or under regulated, so it's encouraging to see it being taken seriously.

Should proposals become regulation in the UK, many MSPs will be forced to re-evaluate their operations and make changes to ensure they have the appropriate cyber security controls in place to reduce the risks to their customers.

A survey completed by the UK Government's Department for Digital, Culture, Media & Sport in May 2021 highlighted how the reliance on MSPs is leading to increased attack surfaces for companies. Respondents also stated that MSPs can represent a systemic risk to the economy due to their scale and concentration of services in the UK market. With change needed, 82 percent of respondents stated that the development of new or updated legislation would be at least somewhat effective, while a further 48 percent deemed legislation to be at least very effective.

Without effective security practices in place, any cyber attack on an MSP can have ramifications for both the firms targeted and their partners or clients across the supply chain. This has become evident over the last couple of years with the rise of supply chain attacks, including the sophisticated nation-state attack against networking tools vendor SolarWinds. More than 18,000 customers were exposed after using SolarWinds' breached software, resulting in governmental agencies and top enterprises suffering targeted attacks. This trend shows no sign of slowing down through 2022 and beyond.

With potential regulation on the horizon in the UK, it's critical MSPs act now and implement robust cyber security measures focusing on separation of duties and reducing their attack surface. Threat Intelligence should be used across all areas of leadership and cyber security to prioritise activity and provide an insight into the risks. Models such as zero-trust and 24/7 threat detection and response should also be leveraged to stop software, services and infrastructure being used to breach customer data. The latter of which should also be integrated into incident response plans and tested using tabletop exercises or breach and attack simulation.

Other proposed changes in NIS 2 include the mandatory disclosing of cyber attacks – something that would impact all sectors. While this might seem like a mammoth task for organisations to undertake, it will be possible as long as the Competent Authorities (CA) ensure the necessary mechanisms are in place to make it happen, such as points of contact to receive and review any incidents. The CA will also need to define templates for initial reporting, which should then be followed up by each regulator after initial review. With CNI crucial to livelihoods, reporting needs to cover whether any incident could affect safety operations, with initial details giving sufficient information to understand the preliminary impact.

IT'S CRUCIAL THAT ORGANISATIONS FULLY UNDERSTAND WHAT THEY NEED TO REPORT

The additional requirements on organisations will depend on the definition of a cyber attack. While there are many definitions of a cyber security incident in national standards such as NIST or the ISO2700X series, requirements will need to be clear. Many cyber security teams identify hundreds of incidents in Security Information and Event Monitoring (SIEM) technologies each month, most of which if not developed correctly, will be false positives or low risk, contained threats. It's therefore crucial that organisations understand what they need to report, or regulators run the risk of inundating regulators with vast amounts of useless data.

Time-bound reporting will also be beneficial as it removes ambiguity about when to report, ensures any trends or themes can be identified for historical purpose and will guarantee organisations can respond in a timely manner. Fast disclosures from time-bound reporting will also allow the CA that is notified of the incident to develop threat intelligence that can be shared with the wider community if it is deemed relevant, which will help protect others in the industry.

The new proposed legislation purely sets out the high-level legal requirements. It does not cover how these cyber security capabilities will be achieved, managed and maintained. Success will depend on the CAs and their approach for ensuring cyber security oversight against the Regulation/Directive.

Disclosing such attacks purely on the basis of the outcome also leaves room for interpretation, particularly as the definition of 'substantial impact' is likely to differ greatly from company to company. Removing this level of ambiguity and streamlining reporting obligations will help to minimise the risk of critical intelligence being missed.

Many UK organisations are adopting principles based on the NCSC's Cyber Security Assessment Framework (CAF) to help ensure best practice security. But they also need to be aware that frameworks used can typically lack security requirements around application development and container-based technologies.

We also need to ensure we don't run before we can walk. In the CNI sector alone, there's still a significant amount of work to be done in order to

ensure all organisations can meet current as well as proposed increased security requirements. In fact, Bridewell research found that over half (55 percent) of organisations are struggling to implement the current framework.

Many sectors are currently on a maturity journey and are typically undergoing various forms of digital transformation to improve security, while ensuring the stability and operation of critical safety systems. This is also compounded with resource challenges and growing levels of burnout that is putting unwelcome pressure on the industry.

THE NIS DIRECTIVE HAS BEEN FUNDAMENTAL IN CYBER RESILIENCE AND MANAGEMENT OF RISK

A better outcome can be achieved across the industry by focusing current attention on improving cyber security against the current requirements as a starting point, before enabling a steady maturity against any new requirements.

Positively, progress is being made. As the UK's CNI becomes increasingly interconnected and interdependent, the government is incorporating The Criticalities Process to better collect the data, with the CNI Knowledge Base being built to better visualise and interrogate the data being produced.

Advances in technology and legislation are helping to improve cyber resilience and drive significant improvements in governance, identification and management of cyber risks and technical defence. However, the problem is that many organisations are unable to make required changes due to operational and technical complexities and risks, which are balanced against the requirement of system up-time.

As operations increasingly shift to the cloud and the introduction of IoT, 5G and machine learning increases connectivity between devices and system, the complexity of cyber security will only increase. Data from IBM's Cost of Data Breach Report highlights that cloud misconfiguration is still one of the most successful attack vectors for cyber attackers. And even for organisations without data on third-party servers, the adoption of cloud platforms like Office 365, Salesforce or Gmail has extended risk profiles, making the role of MSPs even more critical.

On the whole, the proposed changes for both the NIS Directive and UK NIS Regulations appear positive, however the challenge will be how that moves from legislative changes, through to practical implementation across each industry, all of which are at varying stages of maturity. Stricter enforcement is good as long as it doesn't see companies being forced into unnecessary cyber security controls by Competent Authorities (CAs) without a full understanding of the ramifications.

While Brexit may serve to complicate matters when it comes to UK and EU matters, it's likely that the UK will align to a European approach. However, the separation from the EU will limit the talent pool available for some UK organisations as EU nationals chose not to work within the UK, expediting the shortage of skills. This strengthens the need for organisations, particularly in CNI to partner with an organisation to deliver an effective Hybrid security operations strategy (SOC) ●

Martin Riley, Director of Managed Security Services at Bridewell

A cyber attack on an MSP can have ramifications for both those targeted and their partners or clients

Picture credit: shutterstock.com