NIS2 still a mystery to a significant minority of cybersecurity bosses at organisations likely to be in scope – research

Cheltenham, UK – 20th November 2024 – Senior cybersecurity professionals at more than a fifth of the UK's largest businesses are – still – "not sure" whether the EU's NIS2 directive even applies to their organisation, new research by specialist cybersecurity consultancy Green Raven Limited has revealed. More than two-thirds of respondents at organisations with at least 1000 employees said that NIS2 does apply to them, but almost 10% of these admitted that their organisation was not compliant as of the October 17th deadline – with a further 3% not sure.

The findings contradict previous research* from June 2024, in which 97% of IT leaders at UK companies declared themselves confident that they would be, or already were, NIS2-compliant.

Morten Mjels, CEO of Green Raven Limited, said: "NIS2 came into force in January 2023 – almost two years ago – so for senior cybersecurity professionals at the companies most likely to be impacted to not know if it even applies… wow. Saying yes, we're compliant may be acceptable; admitting that no, we're not compliant but we're working on it may also be acceptable– assuming there may be a grace period when new regulations come into force.

"But, eventually, failure to be compliant is going to significantly impact the ability of these organisations to do business in Europe or is going to attract a significant fine for doing business in Europe without being compliant. And saying 'we weren't sure' is unlikely to be much of a defence," he added.

The research also asked respondents for their reaction to the Cyber Security and Resilience Bill, trailed by the UK Government in July 2024's King's Speech. This new bill is expected to build upon the foundations laid by the EU's Network and Information Systems (NIS) directive and is commonly seen as the UK's response to the NIS2 directive.

Asked to react based on what they had heard or read about the new Act:

- **37%** of respondents hope that the new Cyber Security and Resilience Bill won't apply to their organisation, but almost 80% expect that it will.
- **46%** of respondents expect the bill to make unwanted demands of UK businesses, but over **82%** expected the bill to make reasonable demands of UK businesses. A similar proportion agreed that the bill would make necessary demands of UK businesses.
- almost **88%** of respondents agreed with the statement "The UK Cyber Security and Resilience Bill will improve the UK's overall cyber resilience". Not a single respondent disagreed with the statement, despite the acknowledgement of the additional demands and overheads the new bill is likely to bring.

Mjels commented: “While few details are known beyond the idea that it will be the UK’s equivalent of NIS2, the key takeaway from the research is that every cybersecurity professional asked clearly believes that there is more that organisations can, and will, be forced – via legislation – to do to improve their cybersecurity posture and resilience. As a cybersecurity professional in an organisation likely to be in scope, I wouldn’t be waiting for legislation.”

Conducted on its behalf by research specialist Censuswide, Green Raven surveyed 200 respondents from among the UK’s 1,930 organisations with at least 1000 employees. All respondents described their role as CISO/director/head/manager of [in] their organisation's cybersecurity team.

The EU’s Network and Information Security Directive (NIS2) aims to improve the overall level of cyber security and standardise cyber resilience across the EU, by requiring operators of critical infrastructure and essential services to implement appropriate security measures and report any incidents to the relevant authorities. EU member states were required to transpose NIS2 into their national legislation by 17th October 2024. Although the UK has left the EU, NIS2 impacts UK organisations that fall under its scope and conduct business in the EU, either as a customer or as a supplier.

Green Raven is a specialist cybersecurity consultancy and reseller, applying decades of track record, experience and knowledge to bring together customers and cybersecurity solution providers. In particular, Green Raven is a white-label partner for Darkscope, the world’s premier predictive cyber threat intelligence for enterprises. Green Raven’s implementation of Darkscope’s unique, award-winning, AI-powered portfolio of solutions spots cyberattacks that others can’t, and before they take place – so those responsible for cybersecurity can reinforce their cyber defences where they know they’re *about* to be needed.

Its Supply Chain Monitoring Service leverages advanced cyber intelligence techniques and cutting-edge technologies to provide comprehensive oversight of an entire supply chain network – a key objective of the NIS2 directive.

[ends]

*Previous research referenced**.**

Notes to editors

NIS2 Directive Fines
Essential Entities (EE) Includes public and private companies in sectors such as transport, finance, energy, water, space, health, public administration and digital infrastructure. Fine level: €10m or 2% of global annual revenue.

Important Entities (IE) Includes public and private companies in sectors such as foods, digital providers, chemicals, postal services, waste management, research, manufacturing. Fine level: €7m or 1.4% of global annual revenue.

Media contacts
Rose Ross/Sarah Olney Ross
rose@omarketing.com/sarah@omarketing.com