RISING CONFIDENCE

Anthony Young *assesses the cyber security risks to the UK's critical national infrastructure*

As cyber threats become more frequent and sophisticated, many of the UK's critical national infrastructure (CNI) organisations are adopting best-practice approaches and growing more confident in their defences. These findings are drawn from recent Bridewell research, which surveyed 521 senior cyber security decision makers across CNI sectors, including communications, utilities, finance, government, transport and aviation. The research found more than eight-in-ten organisations have implemented (or plan to within 24 months) innovative approaches such as hybrid security operations centres, or managed detection and response.

Morale is also on the rise. The percentage of respondents expressing confidence in the security of their IT rose by 8 percent from last year, both in IT and operational technology (OT). More than 80 percent of respondents are confident about the security of end-user devices, identity providers, cloud or on-premises infrastructure, and SaaS applications. Yet, while confidence has grown, organisations can't afford to become complacent. With tighter budgets, rising AI threats, and government warnings about nation-state activity, staying vigilant is more important than ever. In this article, we'll explore the key insights from our research, focusing on the major challenges and opportunities for CNI organisations to enhance their cyber defences.

Much of the confidence we're seeing likely comes from the significant drop in the number of cyber attacks that respondents reported over the past year. The research found a 71 percent year-on-year drop in reported nation-state attacks in 2023. Ransomware, supply chain attacks, the exploitation of unpatched vulnerabilities and employee sabotage were all down by 61 percent. The average numbers of these incidents were in single figures.

The fall in nation-state attacks may reflect a closer focus by Russia and Iran on the US and the conflicts in the Ukraine and Middle East. Yet by their very nature, these types of attacks are very complex and therefore very difficult to attribute. Any judgment on the matter involves a degree of subjectivity.

The authorities see no let-up in nation-state activity. Last year, for example, the NCSC (National Cyber Security Centre) issued a notice about the danger of China state-sponsored activity against US CNI, warning these techniques could be applied elsewhere. The potential, the NCSC believes, is for destruction, rather than mere disruption. In the US, the FBI similarly believes much of the China-originated cyber activity against CNI is preparatory work in the event of a more serious confrontation.

The UK CNI sector must question whether faith in existing protection is reliant on poor-quality detection and deficient toolsets, along with inadequate threat intelligence. Poor threat intelligence can easily give a false impression of what CNI organisations face or have experienced. It's therefore crucial for organisations to continuously improve their threat intelligence capabilities, ensuring they are using the most effective detection tools available.

It's vital that organisations continue to improve their threat intelligence capabilities, ensuring they are using the most effective detection tools available

Despite the improvements and increased confidence, almost all respondents (98 percent) reported facing significant security challenges. Many concerns are mounting, as organisations continue to struggle with familiar threats and challenges. Malware, for example, is still the most-frequently cited threat to IT and OT environments (by 36 and 32 percent of respondents, respectively).

Data protection and privacy increased as a challenge by 106 percent year-on-year, cited by 37 percent of respondents. Concerns about cyber security tools shot up 121 percent year-on-year. Worries about cyber security tools increased in the course of last year when the NCSC warned of the subversion of "built-in network administration tools on targets' systems to evade detection after an initial compromise".

To combat malware, organisations should invest in advanced threat detection tools and regularly update systems. For data protection and privacy, frequent audits and encryption practices are essential. Reconsidering risk assessments with an attack-vector focus can also uncover potential lateral movement pathways into critical environments.

Building on the challenges of malware, ransomware continues to be a formidable threat, with the growth of Ransomware-as-a-Service and the use of AI in adaptive attacks. The NCSC stresses that ransomware criminals bent on financial gain are serious adversaries for CNI cyber professionals in terms of the volume of attacks they launch.

Some 60 percent of CNI respondents' organisations suffered a ransomware attack last year, with disruption, loss of revenue from downtime and loss of data the three most commonly cited consequences. The average cost of a ransomware attack in the research is also close to £300,000, but it is worth remembering that the Black Basta gang inflicted costs anywhere between £15 and £20-million on the outsourcing company Capita in 2023. What is striking is that 30 percent paid a ransom, which is a risky practice given the danger of infringing strict US, UK and EU rules about payments to sanctioned individuals.

To effectively combat the ransomware threat, organisations should invest in comprehensive backup solutions, conduct regular security training

ORGANISATIONS SHOULD FOCUS ON LEVERAGING AI TO ENHANCE EXISTING SECURITY MEASURES

and implement advanced threat detection systems. Establishing clear protocols for incident response and ensuring all employees are trained to follow them can significantly reduce the impact of an attack.

Supply chain attacks have become a significant concern for CNI organisations. Fears have grown ever since the SolarWinds attack in 2020 and the Kaseya breach of 2021. Overall, our research found 88 percent of UK CNI organisations experienced a supply chain attack in 2023, successful or not. They took various forms, including firmware attacks, compromise of software suppliers and data interception or tampering. Despite these challenges, confidence in the ability to deal with these types of attacks remains relatively high. 83 percent of respondents say they are either very or somewhat confident.

To effectively combat supply chain attacks, CNI organisations must adopt a comprehensive supplier assurance framework. While many enterprises already have such frameworks in place, they often can be treated as a tick-box exercise, gaining false assurance from suppliers merely being ISO 27001 certified or claiming to have various security controls. The information provided is frequently unverified.

Companies need to focus on third parties that pose the greatest risk if compromised by conducting thorough business impact assessments. They should verify security controls as they pertain specifically to their interaction with the business, rather than relying on automated third-party assurance tools or broad security certificates like ISO 27001. This hands-on verification approach ensures a more accurate and relevant assessment of supplier security.

With threats constantly shifting in scale and methodology, conventional preventive tools need to be combined with more comprehensive approaches. The signs here are positive. Over 85 percent of organisations are implementing – or plan to implement within the next few years – measures such as audited security management systems for IT and OT. Additionally, many are adopting 24/7 monitoring and hybrid security operations centre services. The AI arms race is already in full operation, with

almost all respondents saying their organisation deploys AI tools. But more than three-quarters are rightly concerned about criminals using the technology in phishing attacks and to enhance exploit development or power adaptive forms of attack and automated hacking.

AI, however, is set to provide a potent toolset to support detection of malicious activity, capable of spotting anomalies and suspicious behaviour from masses of data. Hype has unfortunately led to AI-badging of entirely conventional cyber detection tools. There is in fact no substitute for the combination of human cyber expertise fully integrated with cutting-edge technology.

CNI ORGANISATIONS NEED TO ADOPT A COMPREHENSIVE SUPPLIER ASSURANCE FRAMEWORK

Organisations should focus on leveraging AI to enhance their existing security measures, while ensuring that human expertise remains central to their cyber security strategies. By doing so, they can better anticipate and respond to the evolving threat landscape.

While organisations are adopting innovative approaches and tools to bolster security, they are simultaneously grappling with budget constraints. Last year, cyber security budgets were down by double-digit percentages, attributed to high interest rates, inflation and economic slowdowns. Across IT and OT, reductions hit spending on in-house staff, risk assessments and risk management, vulnerability management and security monitoring, managed services and tooling.

Spending is only set to increase by less than three percent on average. When it comes to filling the long-established cyber skills gap, organisations are sticking to the tried-and-tested such as recruitment agencies and apprenticeships, but more of them are interested in reskilling current employees than last year (43 percent compared with 36 percent) and there is a slight increase in the use of outsourced partners and suppliers.

The need to meet changing regulatory requirements may force the hand of those in charge of budgets. Regulatory change is one of the main drivers of cyber maturity in the 2024 research, cited by more respondents than evolving threats or the need to support new technology and digital initiatives. Regulation and cyber security go hand-in-hand of course. Many organisations still have a way to go on compliance with regulation such as the NIS regulation, GDPR, EU Cyber Resilience Act when it comes into force and DORA standards.

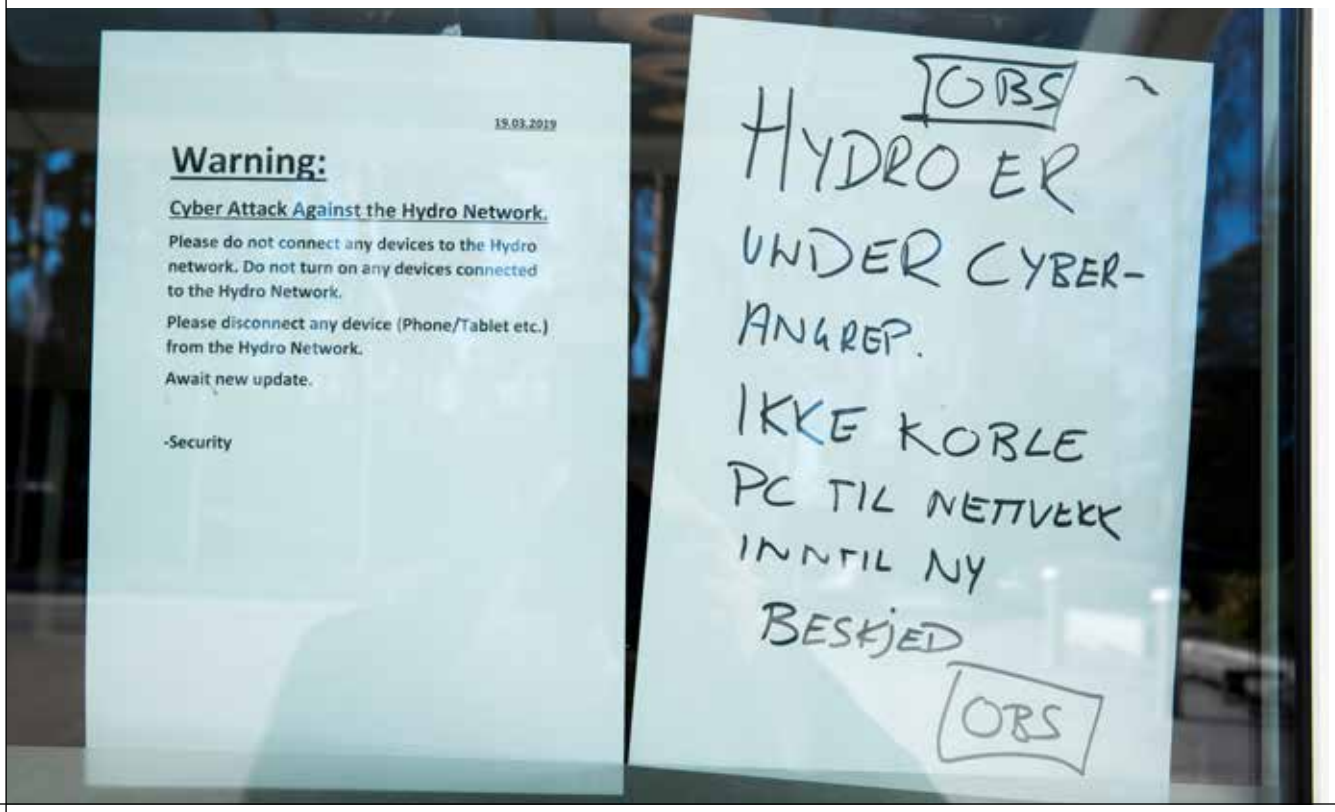
To navigate these financial constraints while enhancing cyber security practices, organisations must prioritise strategic investments, focus on training and reskilling, and stay ahead of regulatory changes. All will be key to maintaining defences.

The research highlighted how CNI entities are aware they face a very broad range of evolving threats. Confidence is relatively high, some of the right steps have been taken with technology and approaches, and organisations feel positive about IT and OT protection despite budget cuts that may well have an effect over the next 12 months. Yet, given the emergence of AI-powered threats and what is likely to be increased nation-state activity, it is vital to strengthen defences even further. Organisations should focus on accessing high levels of cyber skills and seek to use threat intelligence to take the initiative. Acting rapidly is crucial, to prevent significant damage.

Alongside the threats from nation-state groups, organisations must not overlook the fact that financial gain remains a major motivation among cyber criminals. Ransomware, malware, data theft and phishing are significant threats. Whatever the nature of the threat, the costs will be very high if CNI organisations fail to devote the maximum resources possible to cyber security ●

Anthony Young
is Founder & Chief Executive Officer at Bridewell.

Ransomware, supply chain attacks, the exploitation of unpatched vulnerabilities and employee sabotage are all down by 61 percent



Picture credit: Getty Images