GRINDING TO A HALT

Joseph Carson *addresses the growing cyber threats to critical national infrastructure*

In an era where digital connectivity underpins the very fabric of society, the security of our Critical National Infrastructure (CNI) has never been more important. In recent years there has been a surge in sophisticated cyber attacks targeting these vital systems, including energy grids, transportation networks and water supply systems. Analysis from Microsoft in October 2023 found that 41 percent of all the threat alerts it sent out in the last year concerned CNI operators.

It's a threat that is being taken seriously by most governments around the world as regulators double down on measures to protect essential services and their connected supply chains. For example, in 2023 the NIS 2 Directive came into effect for member states of the EU, with new requirements for essential and important industries to tackle rising cyber threats.

In the UK, the NCSC has flagged an: "enduring and significant" threat to critical infrastructure in its 2023 annual review, and as the country is now the third for number of cyber attacks, it's no surprise that the Science, Innovation and Technology Select Committee recently launched an inquiry into the cyber resilience of the UK CNI, considering its critical role in supporting and growing the delivery of public services. All organisations within the sector and those in their supply chain must fully understand the nature of the threats they are up against and pursue strategies for enhancing their resilience.

The UK is at high risk of a catastrophic ransomware attack that could bring its CNI to a standstill

The criminal groups targeting the critical infrastructure are formidable opponents. The head of E.ON one of Europe's largest energy suppliers, recently stated his firm has been continually attacked by high-level adversaries and called for states to do more to protect the sector. In the UK a parliamentary report has stated that the UK is at high risk of a "catastrophic" ransomware attack that could bring the country's CNI to a standstill, bringing further scrutiny on the cyber security challenges and measures needed to safeguard these essential services.

The work of nation-state actors has been linked to numerous cyber incidents targeting CNI. The NCSC highlights China, Russia and Iran as the main perpetrators, with objectives ranging from espionage to cyber warfare. Cyber attacks have become a standard element of geopolitical manoeuvring, used for espionage to acquire political and economic secrets. Microsoft's research indicates there has been some decline in destructive attacks in 2023 in favour of more subtle and persistent espionage tactics. Nonetheless, attacks designed primarily to disrupt essential services remain a prominent threat, often serving as an extension of traditional warfare – as we have seen with the conflict in Ukraine.

State-backed groups have the assets and capital to employ advanced persistent threats (APTs) that are complex and stealthy. APTs are designed to infiltrate networks undetected, allowing attackers to maintain a long-term presence within the target infrastructure. This approach enables them to gather intelligence, monitor activities and potentially disrupt operations at a time of their choosing.

While these groups are a grave threat, the UK's CNI also faces threats from criminal gangs motivated primarily by financial gain. To this end, ransomware has now become one of the most common tactics used by these groups, encrypting an organisation's data or systems and demanding payment for their release, or in other cases exfiltrating data and selling it on the Dark Web. They increasingly view CNI as a lucrative target for these attacks as the essential nature of the services allows for significant leverage in ransom demands.

The nature of critical national infrastructure creates many unique challenges that leaves it vulnerable to attack, and one of the most significant is relying on an ageing and legacy technology.

Many systems that are in use across our national infrastructure now interface with modern technologies, creating a patchwork of old and new that is challenging to secure comprehensively. This juxtaposition of legacy systems with modern IT assets introduces unique vulnerabilities, making them attractive targets for cyber adversaries.

The convergence of traditional IT and Operational Technology (OT) further complicates the security landscape. Many organisations across all CNI sectors – from energy providers to water companies, telecoms companies and emergency services – heavily depend on OT assets such as industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and programmable logic controllers (PLCs) that were designed in a pre-digital era. And where Internet of Things (IoT) devices – such as smart sensors in energy grids or automated control systems in water treatment facilities – have been deployed, in many cases they offer minimal security features. These systems are rarely designed to mesh with standard security controls. As organisations within the CNI embrace a programme of digital transformation as it is beneficial for operational efficiency, the boundaries between IT and OT blur, leading to an expanded attack surface, with critical systems exposed and unprotected devices that can be exploited as entry points into broader network systems.

Addressing these key risk factors requires a security approach that is as dynamic and multifaceted as the sector's threats.

THE CONVERGENCE OF IT AND OT SYSTEMS HAS EXPANDED THE THREAT LANDSCAPE

Although CNI security strategies must encompass a comprehensive approach addressing both technological and human factors, a strong cyber security posture in CNI involves building good foundations, including regular vulnerability assessments and penetration testing, particularly focusing on the interfaces between IT and OT systems. Ensuring that security patches are applied promptly, and systems are kept up to date is vital, as well as implementing network segmentation to limit the spread of a cyber attacks within the infrastructure.

Of course, getting the fundamentals right is not enough and organisations should explore more advanced technology opportunities, such as integrating AI and automation into their cyber security strategies. For example, AI-driven tools can help monitor networks for unusual activities, detect anomalies and predict potential threats based on data patterns and algorithms. Automation aids in rapidly responding to incidents, reducing the time between detection and remediation.

The speed and precision of automated, AI-powered tools are particularly valuable for managing CNI's often complex and sprawling IT environments. However, it is essential to maintain a balance as an over-reliance on automated systems without human oversight can lead to gaps in security.

In this AI-era it is worth noting that the human element in cyber security still plays a crucial part in prevention. In fact, Verizon's Data Breach Investigations 2022 Report has stated that 82 percent of all data breaches involved a human element. Training staff to recognise and respond to cyber threats is fundamental, which includes building their awareness of phishing attempts and understanding the importance of strong password policies. Equally important is establishing a culture of cyber security within the organisation, where security is firstly and foremost seen as a collective responsibility that stems from internal practices. Finally, even with well-layered defence, no system can ever be fully impenetrable, so having a well-defined incident response plan is essential. This should outline clear protocols for responding to different types of cyber incidents, roles and responsibilities during an incident.

By combining these strategies, CNI organisations can create a resilient defence against the evolving landscape

of cyber threats. This resilience is not just about preventing attacks but also about having the capability to quickly recover and restore normal operations in the event of a breach.

Effectively applying these security measures hinges on organisations' first identifying and prioritising the most critical assets in their IT environment. This requires mapping the network infrastructure to understand where the most sensitive and essential data and services reside. Once identified, these assets require stringent protective measures, including advanced encryption, access controls and continuous monitoring for potential threats.

The next step is identifying and neutralising the most prevalent threats to them. Regular penetration testing, especially in OT environments, identifies vulnerabilities that might not be apparent in day-to-day operations. Given the unique challenges in OT environments, such as legacy systems and the need for uninterrupted operations, a specialist approach to penetration testing is required. This ensures that security assessments are thorough yet do not disrupt critical processes.

Similarly, the convergence of IT and OT systems has expanded the threat landscape. Establishing better security for both environments requires both technological integration and a unified approach to risk management. This includes shared policies, procedures and a common understanding of the risk landscape. IT and OT teams need to be in regular communication, working together to spot any necessary changes or issues with their infrastructure, rather than the heavily siloed approach that is common today.

One of the most important factors is managing how these environments are accessed. Both Identity and Access Management (IAM) and Privileged Access Management (PAM) are critical in controlling network systems and data access. IAM ensures that only authorised individuals have access to specific resources, while PAM provides an additional layer of security for accounts with elevated access privileges. Implementing these systems helps mitigate insider threats and risks from compromised user credentials.

CNI operators should also be prepared for the worst-case scenario of a major breach and transparency in identifying and reporting cyber incidents is vital for all organisations within this sector. The forthcoming NIS2 directive requires a 24-hour turnaround for severe incidents, for example.

Disclosing incidents responsibly also demonstrates to stakeholders that cyber security practices are being followed and threats are being taken seriously. CNI sectors would also benefit from a more open approach to sharing lessons learned with the wider community to prevent similar attacks.

As the NCSC's review has flagged, environments with increasing levels of digitisation and complexity progressively become highly vulnerable to attack and more must be done on a national level to safeguard the UK's infrastructure.

All critical infrastructures face an evolving landscape of cyber threats, carried out by sophisticated, well-resourced nation-state actors and increasingly agile, brazen criminal gangs. Defending them requires individual operators and central government having a concerted, proactive and dynamic approach to security, based on fortifying defences and fostering a culture of vigilance and continuous improvement. Given that any attack on these vital services has the potential to bring a country to a standstill, operators also need full national support in defending against these threats. Governments must continue collaborating with security leaders to share intelligence, best practices and adapt regulatory frameworks to keep up with increasingly bold and devious adversaries ●

Joseph Carson is Chief Security Scientist (CSS) & Advisory CISO at Delinea.

CNI faces threats from criminal gangs motivated primarily by financial gain