National Protective Security Authority
Personnel Security: One Small Step
Security measures needn't cost the Earth
National Protective Security Authority
Contact your organisation's security department or speak to your manager
© Crown Copyright
National Protective Security Authority
Personnel Security Your Company Needs You
Security is everybody's business
National Protective Security Authority
Personnel Security Fly in the Ointment
Management responsiblity for employee risk

Picture credit: Crown Copyright

FIGHTING BACK

Martin Riley *reveals what the launch Launch of the NPSA means for organisations in an era of state-sponsored cyber threats*

The NPSA was set up in March to address the growing nation-state threat of espionage, terrorism and other forms of malicious activity directed at businesses and organisations

State-sponsored cyber attacks have shifted up a gear in recent years, forcing global authorities to proactively evolve their defence capabilities. In March 2023, the UK government announced the launch of a new intelligence body, the National Protective Security Authority (NPSA). The agency, which is part of MI5, seeks to address the growing nation-state threat of espionage, terrorism, and other forms of malicious activity directed at businesses and organisations.

Revealingly, the NPSA has already absorbed the responsibilities of the Centre for the Protection of National Infrastructure (CPNI) with a 'broader remit' beyond critical national infrastructure (CNI). While protecting UK CNI will continue to be a key focus of its work, this shift reflects the rising scope and breadth of security threats facing all organisations – from science and technology startups to event venues, universities and research institutions.

In today's turbulent geopolitical landscape, cyber security issues have been elevated to issues of national security. The formation of the NPSA comes amidst an escalation in nation-state cyber crime following last year's Russian invasion of Ukraine, with 72 percent of cyber security decision-makers across UK infrastructure reporting a rise in cyber attacks since the start of the war. As military conflict continues to shift beyond the battlefield and into cyber space, Russia and other nation states are also evolving their tactics to steal intellectual property for competitive and national advantage.

So, as this new security agency begins life, what will be the impact of the NPSA's creation? Most importantly, how can it help businesses and organisations build resilience against ever-evolving national security threats?

To some degree, the NPSA may be seen to overlap with existing functions in GCHQ, such as the National Cyber Security Centre (NCSC). Like other bodies within the UK's intelligence and security agency, the NPSA will provide advice and guidance on cyber security issues to a wide range of sectors, helping organisations to better protect themselves and maintain their competitive advantage.

However, the focus of this new agency is more targeted, centring on the espionage activities and associated threats from nation states such as China, Russia, Iran and North Korea. Advanced technologies, including cutting-edge cyber tools and technical surveillance equipment, are being deployed by groups within these countries to infiltrate and compromise organisations' systems and networks to gather sensitive information, posing significant challenges to UK national security.

The NPSA therefore should not be considered 'just' another GCHQ function. In fact, its formation is a bellwether for where the cyber landscape is heading. As nation-state actors expand their objectives, intellectual property theft and commercial espionage are being seen as increasingly valuable forms of attack. They can also go unnoticed within a company's environment for very long periods of time, especially if attackers leverage a zero-day vulnerability.

Last year, MI5 and FBI chiefs warned of the growing threat to organisations by espionage, particularly those emanating from China. The Chinese regime has been investing heavily in developing its espionage capabilities over the last decade – and is now widely regarded as the "broadest, most active and persistent" cyber espionage threat to Western nations. There are also fears that China-backed groups may be using techniques such as artificial intelligence (AI) and machine learning (ML) to accelerate their attacks and evade detection.

For UK businesses and organisations, it is important to remember that state-sponsored espionage and intellectual property theft are closely tied to wider global forces and trends, such as the race towards renewable energy. The Chinese state, for example, has a strategic agenda to rapidly develop renewable and sustainable energy, with plans for 33 percent of the country's energy consumption to come from renewables by 2025. Espionage could be playing a part in allowing China to significantly reduce its research time, undermining the efforts of other countries and potentially opening the door to further escalation of nation-state cyber attacks.

The effects of espionage and related cyber threats are wide ranging. Not only could it put lives and livelihoods at risk, but it also weakens UK business and harms competitiveness on the world stage. This highlights the crucial link between cyber security and economic security – one that may become increasingly prevalent due to the ongoing economic downturn and cost-of-living crisis.

Tellingly, Bridewell research reveals that over a third (35 percent) of UK security decision-makers in CNI organisations believe that current economic hardship is causing more internal employees to turn to cyber crime. Vulnerable insiders could be particularly susceptible to the tactics of sophisticated nation-state actors, who may offer them a lucrative payoff in return for access to sensitive data or protected systems.

As such, the NPSA will focus on the wide-ranging threats and vulnerabilities that leave organisations at risk of exploitation such as espionage. These vulnerabilities span from phishing attacks, which compromise end users by tricking them into revealing sensitive information or installing malware, to unsecured endpoints and weak VPN protocols in remote working environments. China-linked hackers are also particularly likely to exploit zero-day flaws to gain quick access to targeted networks.

To strengthen resilience in the face of nation-state espionage threats, organisations should develop a strategic, intelligence-led approach. They must also put the right controls in place to ensure that information, systems and intellectual property are secured and monitored, for a quick response if threats materialise.

ORGANISATIONS CAN TAKE A MORE PROACTIVE APPROACH TO IMPROVING THEIR CYBER SECURITY

While the NPSA has not introduced any regulatory measures, its formation contributes to a bigger picture of greater security oversight in recent years – and a closer alignment between cyber security strategies and compliance priorities. Indeed, strong progress has been made across industries since the introduction of the Network and Information Systems (NIS) Regulations in 2018. The regulations have helped CNI organisations improve their cyber resilience by carrying out regular risk assessments and implementing robust security measures such as security monitoring and network segmentation.

Today, the good practices of NIS Regulations, implemented through the Cyber Assessment Framework (CAF), or standards such as the NIST CSF, still apply to enable organisations to control risk as much as possible. The launch of the NPSA is a complementary measure, helping companies to responsively tailor their risk management processes to new and emerging threats.

For example, the NPSA will provide guidance on how to manage the risks when procuring technology from nation states, highlighting how these technologies may pose a threat to industry from espionage or other surveillance activities. This reflects ongoing concerns about Huawei's involvement in the development of 5G communications networks, with some suggesting that the company's close ties to the Chinese government could pose significant espionage risks. In response, the UK government issued a deadline for the removal of Huawei equipment from all 5G networks – but recently extended it to the end of 2023.

The issue of nation-state espionage goes beyond tech giants like Huawei. To mitigate security risks when buying any technology from nation states, organisations must put appropriate controls in place to protect their supply chain and assess all risks related to funding sources and partners. This will involve driving continuous improvements in supply chain assurance practices and processes, and ensuring active, on-the-ground monitoring of the cyber posture of critical third parties and vendors.

Continuous education is a key pillar of a robust cyber security posture. Accordingly, the NSPA is set to provide joined-up, holistic training and advice on the protective security measures organisations must put in place to prevent terrorist attacks, with an emphasis on the evolving nation-state threats facing the UK. This reflects a growing industry-wide focus on education and training, as the 'human factor' is recognised as a critical component of cyber security. According to IBM, human error contributes to 95 percent of all cyber attacks – and over two-thirds (67 percent) of UK CNI organisations have seen an increased cyber risk from insiders (whether malicious or negligent) in the last three years.

THE FORMATION OF THE NPSA COMES AMIDST AN ESCALATION IN NATION STATE CYBER CRIME

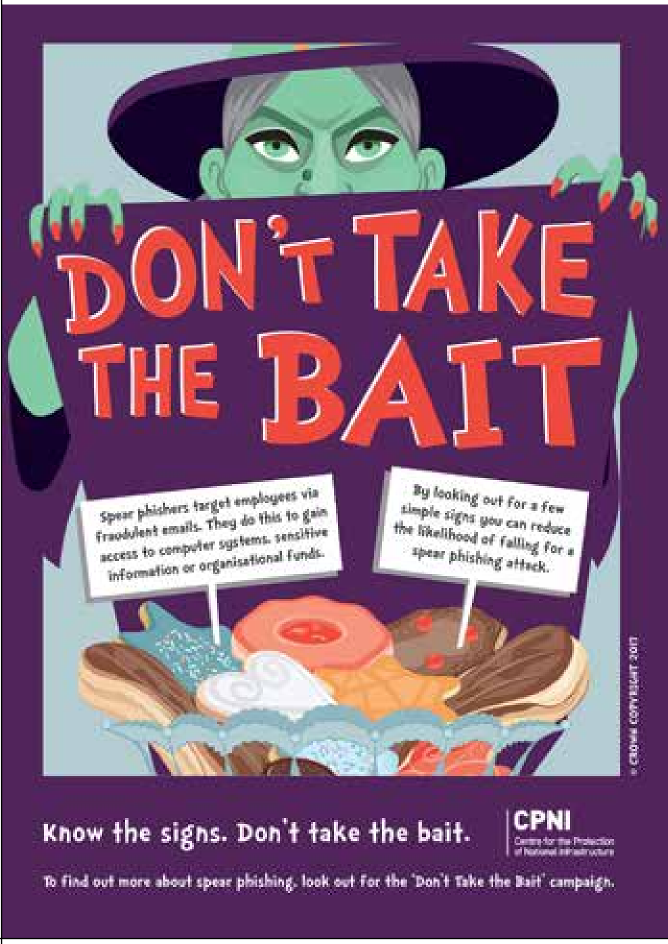
To keep pace with a significantly widened attack surface, organisations must increase the frequency and scope of their cyber security training, integrating education and awareness with their day-to-day operations. We all learn from our mistakes, so regular simulations and practice attacks can be particularly useful in encouraging people to reflect on how they would react to a real nation-state threat. Education should be relevant, up-to-date and varied in deployment to reflect the ever-shifting nature of cyber risks.

Intelligence sharing and collaboration will also be at the heart of the NPSA's security work. Advice will be informed by the latest threat intelligence, alongside active partnerships with security specialists ranging from the police to the NCSC and the National Counter-Terrorism Security Office. With multiple entities pooling their resources and expertise, organisations are empowered to better understand their cyber risk profile and take appropriate measures to prevent or mitigate attacks.

By following the example set by the NPSA and other security partners, organisations have an opportunity to take a more proactive approach to improving their cyber security posture. In particular, the disclosure, consumption, and sharing of timely threat intelligence is fundamental to developing a resilient, threat-led cyber defence capability. Working closely together enables organisations across UK industry to gain better insights into the full spectrum of threats they may face – something that will become increasingly important in the years ahead as nation-state threat actors become more sophisticated, ambitious and well-resourced.

The formation of the NPSA points to the growing severity and scope of national security threats being confronted by UK businesses and organisations. However, despite the increased focus on state-sponsored espionage activities and associated threats, the fundamental components of cyber resilience and security best practice – already implemented through the NCSC's CAF – stand firm. The NPSA will be a complementary force, supporting organisations as they proactively manage nation-state cyber risks through collaboration, threat intelligence sharing and continuous security training and awareness ●

Martin Riley is Director of Managed Security Services at Bridewell

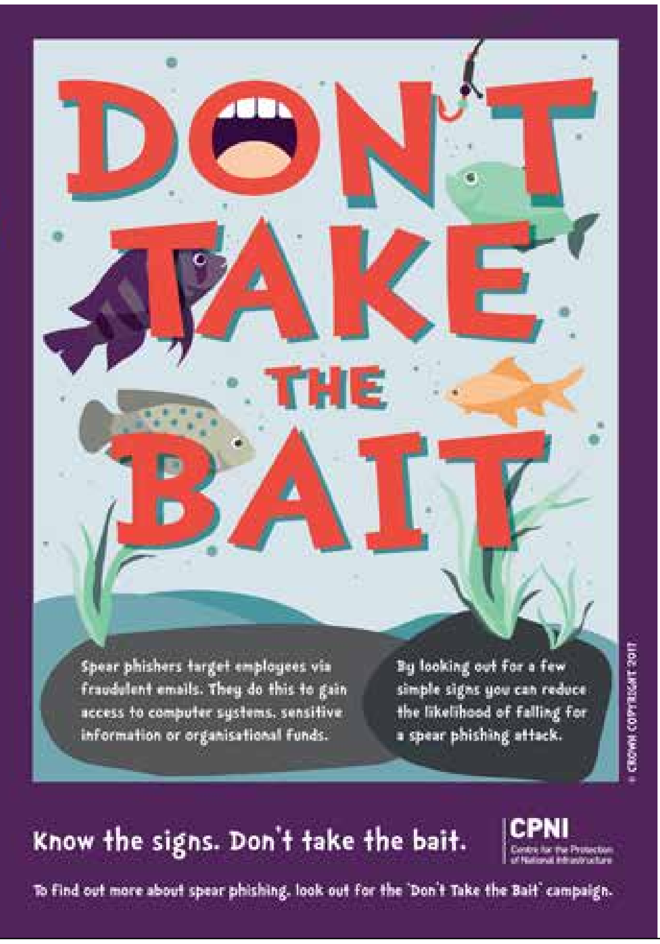


Spear phishers target employees via fraudulent emails. They do this to gain access to computer systems, sensitive information or organisational funds.

By looking out for a few simple signs you can reduce the likelihood of falling for a spear phishing attack.

Know the signs. Don't take the bait.

To find out more about spear phishing, look out for the 'Don't Take the Bait' campaign.



Spear phishers target employees via fraudulent emails. They do this to gain access to computer systems, sensitive information or organisational funds.

By looking out for a few simple signs you can reduce the likelihood of falling for a spear phishing attack.

Know the signs. Don't take the bait.

To find out more about spear phishing, look out for the 'Don't Take the Bait' campaign.

The NPSA provides advice and guidance on cyber security issues to a wide range of sectors

Picture credit: Crown Copyright