POSITIVE IMPACT

Thomas Owen *considers if the NCSC can realistically be considered the equivalent of the NHS for cyber security*

The National Cyber Security Centre (NCSC) has taken a modern, confident and disruptive approach since its founding two years ago, embracing the 'digital' in 'digital government' and, in general curating and delivering positive change for the nation.

It has put a strong emphasis on propagating the long-term skills needed to maintain the UK as a centre of IT excellence, through successful engagement with the public and businesses. It has also done an impressive job in directly cleaning up the UK's IT ecosystem, with cost-effective measures to address 'low-hanging' threats and commodity cyber attacks.

The National Audit Office recently raised concerns with the UK's cyber security efforts, and most security experts agree that not enough is being done to prepare the UK from the emerging digital landscape. However, the NCSC deserves recognition for its innovative approach to building the UK's immunity to cyber threats and responding to cyber security outbreaks; much like an NHS for cyber security.

CISP PROVIDES FREE CRITICAL INTELLIGENCE ON CYBER THREATS IN TIMES OF EMERGENCY

The problem is not so much the NCSC's approach or philosophy, but the volume of its work and inability to reach the nucleus of British business. The NCSC's work should be expanded to better resemble a national digital health-service. This would require greater finances, support and open mindedness from the rest of Government, to allow the NCSC to cater for the full spectrum of British business and develop into a comprehensive provider of healthcare. Here are some areas where we would benefit from NCSC expansion.

Much like Public Health England, the NCSC has proved adept at communicating to a variety of different audiences to change habits that impact the health of the population. One of the most well-regarded projects by the NCSC is its 'Cyber Essentials' scheme, which promotes five basic security controls that will defeat the majority of online attacks; including firewalls, anti-virus, passwords and account management, patch management and basic secure configuration. Originally developed by CESG and the Department for Business, but expanded further by NCSC in recent years, the scheme works much like a public health campaign to promote basic infection control among businesses, with easy to implement controls that are applicable to any kind of organisation, from a local florist to a major corporation.

Despite being voluntary, the scheme has received good uptake from businesses, as it has been intertwined into the Government procurement system and positioned as accreditation of best practice for security. From October 2014, it became mandatory for all suppliers bidding for certain Government contracts to be certified against the scheme, ensuring a commercial driver and an additional incentive for businesses to engage.

BACK TO BASICS

The NCSC also recently published its Board Toolkit to encourage the C-suite to learn about the 'basics' of cyber security. It followed the Government's 2018 Cyber Governance Health Check report which warned of a lack of understanding around cyber threats among senior business leaders.

The Board Toolkit highlights some of the most pertinent areas of cyber security, explains its importance to the board and provides recommendations on what businesses should do to protect themselves. It's an excellent resource for learning and clearly communicates the responsibility of boards to ensure organisational security. Many organisations would benefit from the NCSC expanding this approach further.

Another parallel to the NHS is the NCSC's work to vaccinate the UK against the most prominent health threats. The NCSC has taken a well-prioritised approach in rooting out the most common, low sophistication 'commodity' cyber threats, as evident with its Active Cyber Defence (ACD) programme. The ACD was originally launched at the end of 2016 to protect public sector organisations from cyber attacks in a cost efficient and scalable fashion.

ACD deploys a range of automated measures across the public sector, including: Takedown Service: asking hosting providers to remove websites and content impersonating the UK Government; Mail Check: which makes it harder for criminals to distribute emails that look like they come from a trusted source; Web Check, which helps Government website owners check for common security issues;

Picture credit: Getty

The National Cyber Security Centre is designed to improve Britain's fight against cyber attacks

and Protective Domain Name System (DNS) to block Government users' access to bad websites, such as those known to distribute malware.

Since its launch, the ACD has dramatically reduced the UK's share of visible global phishing attacks, from 5.3 percent in June 2016 to 2.4 percent by July 2018. Between September 2017 and August 2018, the ACD removed 138,398 phishing sites hosted in the UK, according to statistics published by the NCSC.

CHANGING CYBER CRIME

Cyber crime, particularly at low complexity levels, is all about economies of scale and cyber criminals are as vulnerable as any other business to changes in market forces. Initiatives like ACD seek to leverage low-complexity, national scale assets and processes in order to change the black-market economics of cyber crime and make it less cost effective for criminals to operate in the UK. By starving out the low-end of cyber crime, we can then concentrate our resources on the remaining high-value threats. In this way, the NCSC can directly contribute to the security of the majority of UK citizens and the viability of UK SME businesses.

Such is the success of the ACD that the Cyber security Research Group and Policy Institute at King's College London recommended rolling it out to the private sector earlier this year. Taking ACD into the private sector is a great idea. The prospect of the Government positioning aggregated, low-cost cyber security capabilities as a 'public good' in the national interest represents a very exciting and a highly welcome concept.

While the technology underlying ACD might not be new in detail, the scale and the way that the NCSC plans to combine direct, automated relationships with core service providers and free to consume, publicly accessible tooling, when positioned as an innate Government responsibility is revolutionary. This is an area where we would almost certainly benefit from NCSC expansion.

Much like the systems we have in place to contain flu epidemics, we need a systemic response plan to protect the average UK citizen against cyber threats. The NCSC's role as the nation's CERT (Computer Emergency Response Team) is bolstered by the Cyber security Information Sharing Partnership (CiSP), which has greatly improved the UK's performance in this area. CiSP is a confidential forum that allows security professionals across the private and public sector to discuss security concerns in real time. It provides critical intelligence on cyber threats and encourages industry collaboration in times of emergency, such as the 2017 WannaCry outbreak.

Organisations of any size can join CiSP and benefit from free, direct access to top security expertise in times of need. By working with the NCSC via CiSP, businesses can help cleanse UK infrastructure from IT threats and help protect their end users. It's also

an opportunity for organisations to take advantage of a source of high-quality intelligence and put another weapon in its cyber security arsenal, provided for free by the NCSC.

Businesses tend to shy away from collaborating on such matters, but NCSC has done a great job in breaking down the walls of secrecy and creating a remarkably open and valuable service for practitioners. Part of the success is down to NCSC's reassurances that CiSP is a confidential environment, meaning that identifiable data is only shared with regulators under special circumstances. This approach should be continued to win over the confidence and trust of more businesses.

EXPANDING ITS REACH

CiSP should now be expanded to reach a far greater proportion of the UK's IT infrastructure. The NCSC should prioritise recruiting more members, particularly SMEs, to build CiSP as an educational resource in times of calmness and emergency. Further assistance should also be provided to smaller companies and non-security specialists to ensure they understand and are able to implement CiSP's outputs.

The NCSC should not only continue its good work in positioning state-level cyber security as a public good, but formalise it as a responsibility to all citizens. It should follow the recommendation to roll out ACD into the private sector in order to build immunity among the smallest, most vulnerable businesses. It should then take this approach forward by developing more control sets and security products for businesses to adopt. These products should also be kept open source and made easily available to all businesses, with guidance to help SMEs implement the tools into their operations.

SMEs tend to be most vulnerable to cyber attacks, and so any activity that raises their defensive capabilities without increasing costs is highly attractive. Initiatives such as ACD are, unfortunately, also likely to slip under the radar for the majority of smaller businesses, as they often lack the tech-savvy personnel to deliver the change. Unless we can encourage awareness among SMEs, a vulnerable underbelly will continue to exist in the UK, providing a continuing viable market for those wanting to profit from these sorts of attacks.

The NCSC should expand its communication efforts further to facilitate more engagement with SMEs outside of the 'London bubble' and should stretch its engagement to all parts of the country and sectors; in order to resemble a truly national cyber health service.

THE CYBER ESSENTIALS SCHEME PROMOTES FIVE BASIC CONTROLS TO STOP MOST ONLINE ATTACKS

What we need is herd immunity through mass inoculation programmes, where the strength of the population at large protects the weakest members. This requires encouraging digital change among as many organisations as possible and in all aspects of society to strengthen the online eco system. The NCSC has paved the way for the UK to benefit from a unique style of digital Government. But we need more bold action to meet the emerging challenges of cyber security. Its ethos should be publicly updated to reflect this ●

Thomas Owen – Head of Security at Memset – joined Memset in 2014 with a wealth of experience following a security-focussed career with cloud hosting providers and big consultancies.

Just some of the areas that the NCSC's excellent website advises on