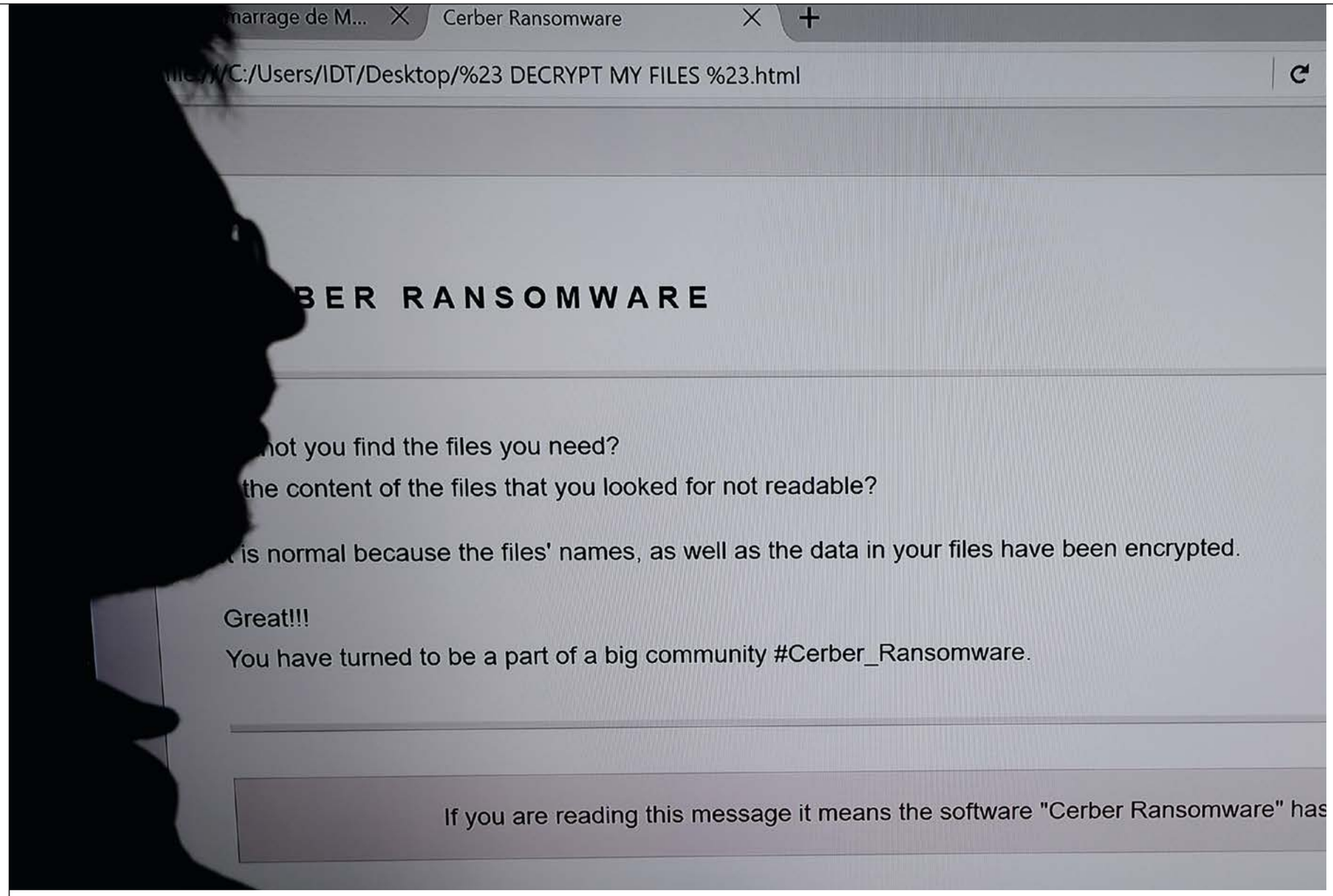

Picture credit: Getty

FACING UP TO CYBER THREATS

Simon Davies *on best practise to avoid the risk of cyber attack*

Cyber attack has been identified as one of the four highest priority and most pervasive of risks faced by the UK – the others being international terrorism, international military crises and major accidents or natural hazards. Data is now vital to everyday business operations and ensuring its confidentiality and security must be of paramount importance to any organisation.

Some £1billion was lost to online crime between March 2015 and March 2016 with seven in 10 business leaders admitting that they have not taken any action to protect their business and employees from financial fraud. It is certain that the future of the UK's security and prosperity will depend on strong digital foundations. The challenge for our generation is to develop a stable digital society that is resilient to cyber threats, and which possesses the knowhow and skills needed to make the most of opportunities and manage risks.

21st-century life is critically dependent on the internet, but it remains inherently insecure and there will always be malicious users eager to exploit weaknesses to launch cyber attacks. Regrettably this threat will always exist to some extent, but the risk can be reduced so that it allows society to continue to prosper and to reap the benefits from the huge opportunities that digital technology brings.

The 2011 National Cyber Security Strategy, backed up by the Government's £860m National Cyber Security Programme, has resulted in major improvements to UK cyber security. It has achieved good results by looking to the market to drive secure cyber behaviours. But this approach has not been successful in achieving the scale and pace of change needed to stay ahead of the fast-moving threat of cyber breaches. Now we need to go further. Last year the Government unveiled a five-year National Cyber Security Strategy and announced it was investing £1.9 billion in defending its systems and infrastructure. It also disclosed it would be setting up a new National Cyber Security Centre that will provide a hub of world-class, user-friendly expertise for businesses and individuals, as well as rapid response to major incidents.

Increasing education to beat the threat of cyber attacks is vital

PROACTIVE TESTING CAN BE BENEFICIAL TO SPOT WEAKNESSES IN NETWORKS

By 2021, the UK must ensure it has the strongest measures in place to defend the country against evolving cyber threats and to respond effectively to incidents. It must make sure networks, data and systems are protected and resilient with citizens, and that businesses and the public sector are equipped with the necessary knowledge and ability to defend themselves.

TOP TARGET

There is no doubt that the UK will be a leading target for all forms of aggression in cyberspace and as a nation we have a responsibility to detect, understand, investigate and disrupt hostile action taken against us, and continue going after offenders and bringing them to justice.

The UK is home to an innovative and ever-increasing cyber security industry, supported by some of the world's best scientific research and development. There is no shortage of experts that possess the skills to meet our national needs in both public and private sectors.

The Government has given its commitment to draw on its capabilities and those of industry to put in place cyber defence measures that boost the levels of cyber security across UK networks. These measures include reducing, as far as possible, the most recurrent types of phishing attacks, filtering known bad IP addresses and blocking malicious online activity. There is no doubt that these improvements in basic cyber security will enhance the UK's resilience to the most commonly deployed cyber threats.

The Government has also stated the importance of the Armed Forces being resilient and supported by the strong cyber defences crucial to securing and defending their networks and platforms. This is of paramount importance so they can be guaranteed the freedom of manoeuvre worldwide despite cyber threats. The military Cyber Security Operations Centre will work closely with the NCSC and ensure that the Armed Forces can provide support should there be a significant national cyber attack.

Increasing education to beat the threat of cyber attacks is also vital, so the Government has taken another positive step by pledging to invest in programmes to address the shortage of cyber security skills in the UK, from schools to universities and across the workforce. This move will be aided by the launch of two new cyber innovation centres to spearhead the development of ground-breaking cyber products and pioneering new cyber security companies. A commitment has also been made to allocate some of the £165m Defence and Cyber Innovation Fund to back innovative procurement in defence and security.

BRIDGING THE GAPS

Much of the hardware and software originally developed to enable an interconnected digital environment has focussed on efficiency, cost and user convenience, but has not always shown the same attention to security. This inherent weakness has allowed malicious users – hostile states, criminal or terrorist organisations and individuals – to exploit the gap between convenience and security. Now bridging that gap is of urgent national importance.

Another major challenge we face is the expansion of the internet beyond computers and mobile phones into other cyber physical or smart systems. Unfortunately, this widens the threat of remote exploitation to many new technologies. Systems and technologies that are part of our daily lives – such as power grids, air traffic control systems, satellites, medical technologies, industrial plants and traffic lights – are all connected to the internet and so can become vulnerable to interference.

The biggest challenge faced by any SME or larger commercial organisation is striking the right balance between security, cost and usability. Any commercial organisation will see the necessity to continue with its work unhindered, but at the same time not make itself vulnerable to something like e-fraud. However brilliantly exclusive a network may be, there is always going to be a threat posed by cyber hackers.

Furthermore, with the ever-changing nature of working practices, fluid movement of personnel, use of mobile devices, cloud services and the Internet of Things, the risks become greater.

As a minimum, you should take steps that include encrypting your data and ensuring your digital perimeter is protected by firewalls, user authentication and other measures to prevent an unauthorised intrusion. Proactive testing can be beneficial to spot weaknesses in networks and procedures, and protect data, to further minimise risk.

If cyber attack has been identified as the most pervasive risk faced by UK companies, are you fully prepared to protect your business from financial loss from theft or fraud, loss of invaluable customer information or intellectual property, possible fines resulting from a breach of data protection or confidentiality regulations, or even a diminished reputation through word of mouth and adverse media coverage?

Cyber attacks cost UK organisations thousands of pounds and can lead to lengthy spells of disruption.

So, what is your plan in the event that your customer database is stolen, your website is forced offline, or you can't access your email or business-critical data?

HELP DESK

For further peace of mind and enhanced security, consideration should be given to the support offered by a Security Operating Centre (SOC), which can provide 24/7/365 monitoring of a network to immediately identify any breach, or potential breach, as well as providing a help desk.

Without doubt, Spectra views cyber security services as the next major growth area. It has already been delivering cyber services through it existing networks business, so the launch of Spectra Cyber Security Solutions is a natural progression for the company.

Developed in conjunction with the Information Security Forum (ISF), the Government-backed Cyber Essentials scheme – which Spectra is fully compliant with – forms a robust and stringent checklist that security companies must meet to be considered eligible to work with highly sensitive information and Government-level security contracts. Spectra is also a Cisco Partner – Cisco Select Certification recognises and rewards partners that have achieved a Cisco specialisation.

Among its staff are experts that possess all the knowhow and experience to deliver highly bespoke security solutions to protect against cyber attacks. It recognises that not every company can afford to have a large, highly trained, IT department, and some need a straightforward pricing system to plan their business operations. Spectra Cyber Security Solutions aims to make keeping companies safe from cyber attack as simple and cost-effective a process as possible.

THE CHALLENGE IS TO DEVELOP A STABLE DIGITAL SOCIETY THAT IS RESILIENT TO CYBER THREATS

Regrettably the threat of cyber hacking is likely to be around for many years to come. The threat itself will just change depending on the technology criminals use to bypass IT systems and software. The likelihood is that the majority of future cyber attacks will continue to exploit basic weaknesses so the objective must be to make networks sufficiently secure to deter all but the most persistent attackers ●

Simon Davies is the CEO of Spectra Group (UK) Ltd. Upon leaving the military in 2004, he established Spectra, which is fast becoming a leading service provider of reliable, robust, deployable communications.

Security of data is of paramount importance to any organisation

Picture credit: Spectra Group