Timothy Compston investigates the growing number of cyber security attacks by individuals and state actors intent on obtaining valuable intellectual property and other sensitive data, and outlines the countermeasures which can stop them

STRENGTHENING CYBER SECURITY

Today cyber attacks are seemingly never far from the headlines in our increasingly interconnected world as organisations report a surge in incidents, with criminals and even, potentially, state actors, seeking to steal industrial secrets on an unprecedented scale, whether that be for commercial or strategic advantage. Information – from advanced aircraft designs to business plans – are now firmly in the hackers' sights; intellectual property that can represent years of effort and millions of pounds worth of investment can be stolen in the blink of an eye. Here we take a closer look at the concrete steps being taken by governments and businesses to mitigate the threat as its implications are more widely understood, and examine why continued vigilance is very much the order of the day.

There is certainly much greater awareness out there of the need for concerted international action, including on the policing front. At the start of this year (January), for example, we witnessed the official launch of the European Cybercrime Centre (EC3). Working out of Europol's headquarters in the Hague, Netherlands, the centre is expected to act as a vital European information hub on all aspects of cybercrime. Moving forward, key tasks for the centre will include: developing and deploying digital forensic capabilities to support investigations in the EU; building capacity by awareness raising and training to combat cybercrime; and supporting best practice. Speaking at the centre's opening, Europol director Rob Wainwright underlined the pressing need for this new resource. "The threats from cybercrime are dynamic and rapidly evolving," he said. "By building trust and establishing information flows between law enforcement and cyber security stakeholders, we will be smarter, faster and stronger, ultimately resulting in a safer cyberspace for EU citizens and businesses."

In April, the UK foreign secretary, William Hague, announced the creation of a Global Centre for Cyber Security Capacity Building in the Oxford Martin School – an interdisciplinary research community – at the University of Oxford as part of the UK's wider National Cyber Security Strategy. The centre, which is supported by government funding of £500,000 per year, has been set-up to take a global lead in the understanding of how to deliver effective cyber security, working with the UK, other countries, organisations and the private sector – a fact which underlines that this is an issue which can no longer be tackled in isolation. By addressing cyber security as a multi-dimensional concept, the centre is planning to consider a wide spectrum of elements, such as: whether it should be tackled at the national or international policy level; people's susceptibility to cyber crime and their attitudes to what is or is not acceptable with regards to the type of risks and the tools to address it; the availability of a skilled cyber security workforce and leadership; the legal and regulatory frameworks; and technologies and standards.

For Sadie Creese, professor of cyber security at the University of Oxford, who heads-up the new centre, this is certainly not an abstract issue but a clear and present danger, with the prospect of cyber attacks on infrastructure being a case in point. "Malicious attacks on our critical national infrastructures are a certainty and have the potential to cause devastating harm; our mission must be to ensure we are prepared and as resilient as possible," she said.

Of course, it is perhaps not surprising that defence companies, which are very much in the sights of cyber attackers as state actors seek to obtain sensitive details on new equipment and weapons systems, want to take their own sector-specific measures. A good example of this trend is the fact that the UK government and a number of defence companies in the UK defence supply chain have come together to create the Defence Cyber Protection Partnership (DCPP), specifically to ramp-up their security and resilience against the higher level cyber threat they face. Members of the partnership will, for example, be able to share threat intelligence and

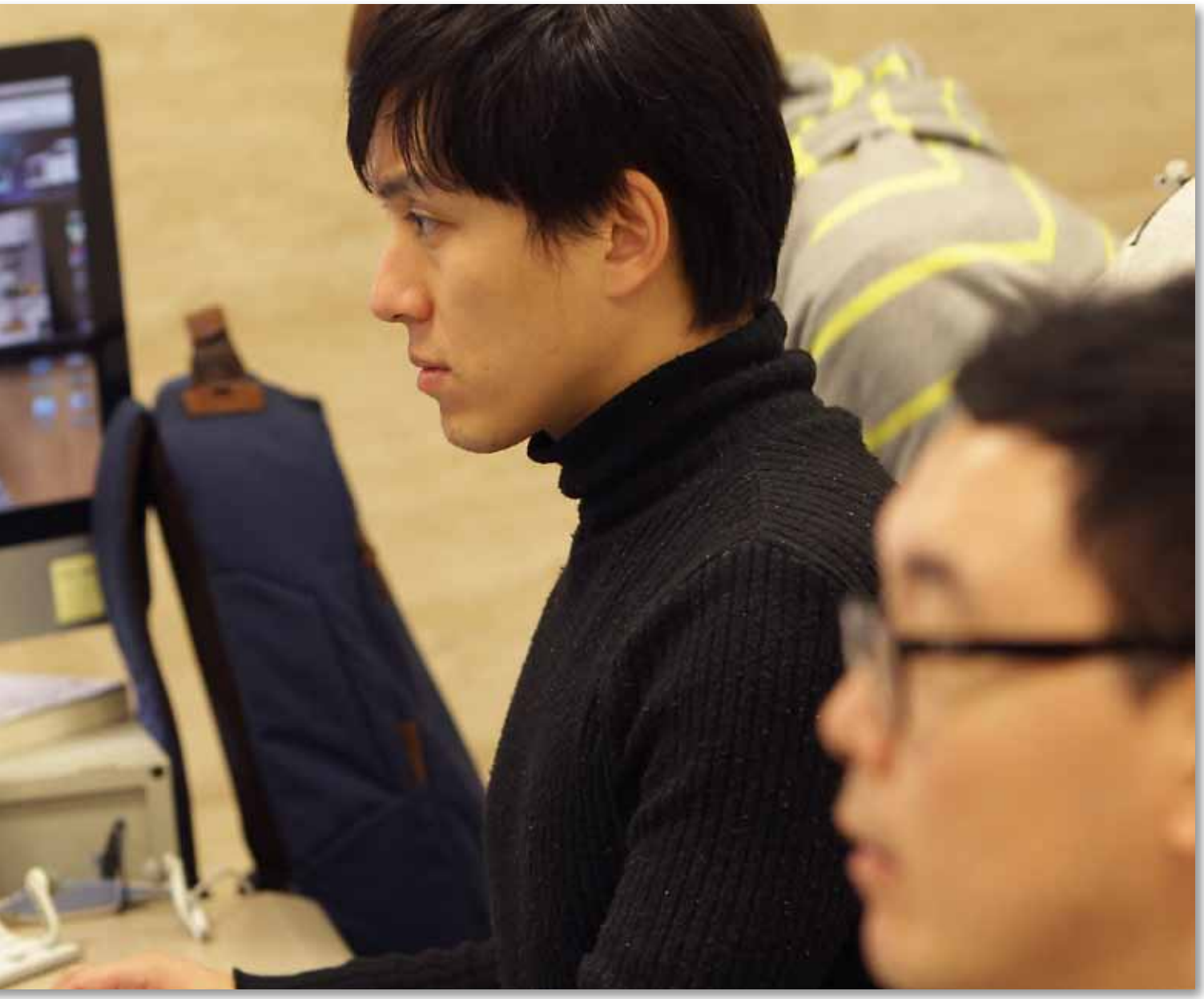
©Getty Images

expertise. The new partnership, announced during the summer, includes the Centre for the Protection of National Infrastructure (CPNI), Government Communications Headquarters (GCHQ), Ministry of Defence and nine companies: BAE Systems, BT, Cassidian, CGI, Hewlett Packard, Lockheed Martin, Rolls-Royce, Selex ES and Thales UK.

On a wider front, business consultancy KPMG recently released a report that hit the headlines by underscoring just how vulnerable businesses are, often unwittingly. Based on an analysis by its cyber response team, KPMG claimed the UK's economic growth and cyber security was actually being put at risk thanks to FTSE350 companies leaving data readily available in the public domain – data that could, potentially, help an attacker to obtain intellectual property, undertake fraudulent activity and cause reputational damage. Significantly, it was revealed that, on average – across the FTSE350 – 41 user names, 44 email addresses and five sensitive internal file locations were readily available for each company.

The KPMG investigation starkly illustrates the need for companies, above and beyond other aspects of cyber-security, to ensure that even at the most basic level they retain effective control over their web presence. Another worrying KPMG finding – which shows the sort of vulnerabilities that hackers are all too happy to take advantage of – was that 53 per cent of the FTSE350 companies had old server software or security patches that were simply not up-to-date.

For his part Mark Brown, director of information security at Ernst & Young, welcomed the UK government's plans to encourage FTSE350 businesses to take part in a cyber health check initiative. "This is the first major step towards taking the theoretical framework that was the Cyber Security for Business Initiative launched in 2012 into practical implementation, and presents businesses with the opportunity to embed cyber checks into their standard corporate behaviour," he said. Brown, however feels that there is no room for complacency, citing Ernst & Young's Global Information Security Survey that revealed a worrying 88 per cent of businesses in the UK reporting an increase in cyber attacks. He also thinks it makes sense to broaden the focus of current plans. "They don't go far enough," he



On guard: South Korean analysts monitor cyber attacks emanating from North Korea

STRENGTHENING CYBER SECURITY

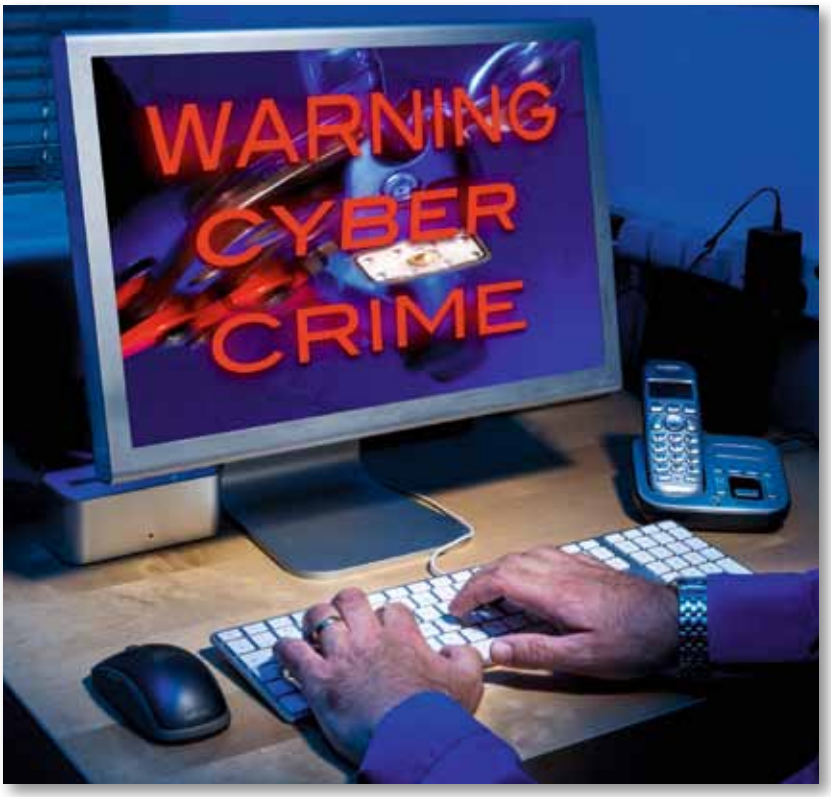
said. "The threat is relevant to, and should be embraced by, the wider business community proportionally. The current plan should expand to include suppliers to FTSE350. This is the only way to ensure their supply chains don't continue to pose an indirect risk to businesses in and out of the index."

In terms of new practical challenges on the ground, Brown emphasised that "the Cloud" and "bring your own device" mobilisation are radically changing the way businesses operate and, consequently, how cyber security is handled. "What businesses are now saying to gain maximum benefit from these new technologies is that, rather than tick a box and say 'our policy says this', or 'you shall not have personal devices', with these new ways of working there are risks which we either have to accept or mitigate.

"So what you are getting, in terms of cyber security, is a recognition that it is not all just about the internal controls around information but the convergence of people, information, operations and brand," continued Brown. Expanding on this, he explained that the reality of an extended enterprise business is that this creates a porous environment where information has to leave the organisation to enable it to operate. "The key thing is for businesses to accept that they are in what I would term an 'assumed state of compromise', and to identify what are the 'crown jewels' that they have to protect, rather than trying to protect 100 per cent of the information 100 per cent of the time," he said. He added that businesses are starting to make conscious decisions that there is some information that doesn't need to be kept secure: "If it is already on the Internet, for example, does it matter?" he asked. "It is about protecting the intellectual capital that actually creates the value within the company."

On another point, Brown also sees plenty of scope for co-operation involving companies and government. "Unlike many aspects of traditional IT heritage where secrecy gives you a competitive advantage because, in many respects, companies are defending against the same common threat, the mechanisms for sharing information and approaches to combating and defending against the threat can be more open," he said.

Given the increasing rivalry between the United States and China, there is growing concern being expressed by lawmakers on the other side of the Atlantic regarding the impact of alleged cyber attacks originating in China, as part of efforts by the world's second largest economy to achieve a commercial or strategic advantage, and the consequences for US companies and the human rights community. In June, Senator Sherrod Brown (D-OH) co-chaired a Congressional-Executive Commission on China (CECC) hearing entitled: "Chinese Hacking: Impact on Human Rights and Commercial Rule of Law". Speaking at the time, Brown certainly didn't pull any punches on the scale of the issue. "China's frequent and illegal cyber attacks have made it the world's biggest violator of intellectual property rights," he said. "The victims of IP theft include companies in Ohio [the state which Brown represents] and hard-working Americans trying to make an honest living, only to see their products, services and technology stolen."



Advanced persistent threat groups can infiltrate corporate networks over a long period of time

Interestingly, the CECC hearing came on the back of a detailed report, issued in February, by cyber security specialist Mandiant – headquartered in Alexandria, Virginia– which highlighted what it claimed was an "espionage campaign" by a large advanced persistent threat (APT) group, stretching over several years. The hard-hitting report, "APTI: Exposing One of China's Cyber Espionage Units", homed in on evidence which in Mandiant's opinion links one group – referred to by Mandiant as "APT1" – to the People's Liberation Army (PLA) General Staff Department's 3rd Department. Apparently, this group alone has been responsible for stealing confidential data from at least 141 organisations since 2006 across a wide spectrum of industries.

Mandiant's chief executive officer, Kevin Mandia, sought to put the actions of "APT1" into a broader context. "APT1 is among dozens of threat groups Mandiant tracks around the world, and one of more than 20 attributed to China that are engaged in computer intrusion activities," he said. "Given the sheer amount of data this particular group has stolen, we decided it was necessary to arm and prepare as many organisations as possible to prevent additional losses."

So, to conclude, it is obvious that the worldwide threat of criminal and state-sponsored cyber attacks is not going to disappear any time soon. This means we are likely to see more industry-specific initiatives similar to those being used in the defence sector, where critical intelligence can be exchanged by those on the front line. We will also see more centres of excellence appearing, such as the Global Centre for Cyber Security Building and Capacity Building, to pool expertise. Crucially, we will see renewed vigilance by businesses to adequately protect their intellectual property wherever they sit in the supply chain.

Timothy Compston is a freelance journalist and PR professional who specialises in security issues. He studied International Relations and Strategic Studies at Lancaster University, is PR director of Compston PR and a previous chairman of both the National PR Committee and CCTV PR Committee of the British Security Industry Association (BSIA).