THE FOUNDATION
FOR SCIENCE AND
TECHNOLOGY

DEBATE SUMMARY

Cyber security: how secure are UK organisations from cyber theft of IP?

Held at The Royal Society on 16th October, 2013

The Foundation is grateful to Jisc for supporting this debate.

The hash tag for this debate is #fstcybersecurity .

Chair: **The Earl of Selborne GBE FRS**
Chairman, The Foundation for Science and Technology

Speakers: **Chief Scientific Adviser**
Centre for the Protection of National Infrastructure (CPNI)
Hugh Eaton OBE
National Security Director, Cisco UK
Professor John V McCanny CBE FRS FREng
Director, Institute of Electronics Communications and Information Technology (ECIT), Principal Investigator, Centre for Secure Information Technologies (CSIT), School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast

---

The CHIEF SCIENTIFIC ADVISER CPNI described the role of the Centre for the Protection of National Infrastructure (CPNI). The Government had divided the national infrastructure into nine sectors, and had identified the critical elements in each, ie those where loss would lead to severe consequences/loss of life. Cyber security constituted an increasingly important aspect.

The threat to UK interests was ongoing and persistent, with the risk of industrial espionage very real. The Foreign Secretary William Hague had stated that the UK was targeted by 1,000 attacks every hour. Typical attacks on companies involved accessing commercially sensitive information, stealing IP, accessing third party data held by UK companies and corrupting data/IT systems to compromise the service.

One of the most common methods was "spear-phishing", in which targeted members of staff were sent credible e-mails with attachments containing malware. It was difficult to estimate the cost of hostile state cyber activity; one company alone had lost around £800 million as a result of a cyber attack. The companies targetted had extended; eg to law firms that advised defence companies. In 2012 a major international law firm had its network compromised in three countries, with valuable information stolen; any client information it held was at risk. CPNI offered: a cyber outreach programme aimed at influencing behaviours at Board level; follow-on support to companies that had been attacked; the enabling of operational capabilities in companies (including through information exchanges, and the Cabinet Office platform for the Cyber-Security Information Sharing Partnership - CISP); advice to companies to better manage the risk themselves; and the launch of a cyber incident response scheme in partnership with CESG and in collaboration with CREST.

The Chief Scientific Adviser CPNI described a case study in which a company had been frequently targeted, and CPNI helped the company work on measures to upgrade its resilience at both a human and technical level. There had, however, been obstacles, in terms of company culture, a resistance by the Board to recognise the risk, resistance to changes, budgetary constraints, and a tendency to prioritise convenience over security. Nonetheless, improvements had been made, though it was still work in progress. In summary, there was no "fix" for the cyber security risk; it was a constantly evolving race.

HUGH EATON said that cyber security would only be enhanced through joint working by

Government, academia and industry. How safe are UK organisations from the theft of their IP? Not very. The threat was not necessarily where one might expect. Criminals went to the places where people went on-line: search engines, advertising and online shopping were especially likely to deliver malware. Sites for prescription drugs and luxury watches were particularly prone.

Criminals also targeted certain times of year, producing malware-containing spam when there was a Microsoft update, in the US tax season, or via professional networks like LinkedIn at times of year when people typically considered a change of career. The attitude of the younger generation to privacy was different; eg in a survey, 3 out of 5 said they did not care about privacy, and 71% said they did not obey company IT security policies. In the public policy area, guidelines and standards were improving.

Companies wanted to know what "good looked like", and the Department for Business, Innovation and Skills was addressing this. Within companies, most CEOs felt that the issue was one for their IT people, without focusing on the fact that it was their business that was at risk. While the larger companies were attacked more, SMEs were also subject to attack. The UK was not uniquely vulnerable.

The police considered that the fall in crime statistics represented a displacement to cyber crime, which was not reported in the statistics. The Home Secretary had said that cyber criminals would be ruthlessly pursued, but it was entirely unclear which authority was equipped to do that. Looking ahead, the political narrative needed tuning, with the police becoming more engaged; a major shift was unlikely unless a major home brand failed; education was, however, leading to stronger defensive measures; and the economic upturn was likely to trail improvements.

PROFESSOR MCCANNY said that 93% of large corporations and 76% of SMEs had reported a breach in cyber security in the last year. The Research Councils were funding an £82m programme across 96 cyber security research programmes, and there was significant additional funding from other national and international sources. There were 11 EPSRC/GCHQ centres of excellence in the UK, plus major research institutes and doctoral training centres.

He outlined the role of his institution: it was badged as a global innovation hub for cyber security, with a focus on network security, data security, cyber physical systems and mobile security. It operated a tiered membership model of open innovation. On data security systems, his team worked on such things as cryptograph algorithms (looking for highly optimised low cost, low power outcomes), side channel attacks, "physical unclonable functions" (circuits with a unique digital fingerprint), and public key infrastructure (eg an anti-tamper device for the infrastructure for charging of electric vehicles).

On mobile network security, they worked on such things as the operating code characteristics of malware (2% of downloads of Android apps contained malware, a doubling over the past 2 years). They had developed links with other institutions globally.

He described the work The Royal Society was undertaking to review cyber security research, aimed at creating a high level vision to help frame a cross sector research agenda, and identify the major research challenges in the next five to ten years. He is chairing the steering committee of the Society for this review. Examples of research challenges identified included privacy/trust, the sustainability of cyber space, bio-inspired analysis of cyber space, privacy and online surveillance, and cyber space in a wider socio-economic context.

In the ensuing discussion the following were the main points:

- In view of the likelihood that businesses would face attacks, what advice was available for resilience and recovery? And how could small businesses be equipped to engage effectively in discussion with companies selling appropriate services without fear of being ripped off? CPNI, with CESG, had been working on identifying and certifying activity by companies that provided resilience and post event advice, and had produced a form of kite-marking. CPNI had also produced guidance notes for addressing the use of the cloud, which was not inherently less secure than other media. The Ministry of Defence were leading work in which a small number of large industrial players determined standards of practice for SMEs in their supply chain. Companies needed protective technology that was smart and cost effective; expenditure on security could not eat up all their profits. Large companies had the resources to address this; indeed, CISCO spent c.£5b pa on trying to improve technology.

- Were companies operating in the UK more at risk than those operating abroad? CPNI was mainly concerned with the operations of companies in the UK, and for example those that experienced regular, persistent attacks. But there was no particular pattern of vulnerability of multinational companies operating in different countries.

- In view of the fact that culture and behaviour of employees was crucial, what could be done to address this? Sets of guidance notes existed, but it inevitably came down to company culture and individual behaviours. Companies needed to recognise that what was written down as company policy was not the end of the matter. It was difficult to run a business that did not share information internally, but not enough thought was given to what needed to be shared and how to do so. In the Bradley Manning case, 250,000 people had had access to the information. It would be interesting to see if companies' recruitment processes could assess aptitude in for example willingness to follow company policies.

- How can public and individual awareness of cyber security be heightened? The further one went from large companies, the harder it was to get the risks understood, and the lack of basic cyber awareness at an individual level was staggering. One idea being pursued was to weave cyber security into the plots of soap operas.

- Was the legal framework fit for purpose? And was there sufficient international collaboration? The idea of an international "law of the ether" was beset with difficulties because of different approaches to norms in different countries.

- Why was industry not developing more routine security for SMEs and individuals; indeed, why wasn't security protection a functionality automatically required by ISPs? There was a ticking time bomb over the arrival of "digital by default" and universal credit. It was pointed out that BT did offer free security provision although only 40% of customers downloaded the software.

- Was it a disadvantage that the UK's "protection" agency, CPNI, had a close working relationship with the "offensive" intelligence agency, GCHQ, unlike the situation in some other countries? There was a positive benefit for CPNI in being connected to the intelligence picture. Was the benefit to the intelligence services of the activities revealed by Snowden offset by the risk that it undermined people's confidence that they could do business in private without surveillance by the authorities? The activities of the agencies in the UK were well regulated.

- The work going on in the UK on cyber security provided opportunities for the UK to be a world leader.

- It was a paradox that, on the one hand, the Government wanted open data from research and yet, on the other, there was excellent work on cyber security being undertaken in our universities which needed protection.

Sir Brian Bender KCB

Ted Talk - Avi Rubin: All your devices can be hacked
www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked.html

Useful links:

Academic centres of excellence in cyber security research
www.epsrc.ac.uk/research/centres/Pages/acecybersecurity.aspx

Centre for the Protection of National Infrastructure (CPNI)
www.cpni.gov.uk

Centre for Secure Information Technologies (CSIT), School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast
www.qub.ac.uk/schools/eeecs/

CESG
www.cesg.gov.uk

Cisco UK
www.cisco.com

CREST
www.crest-approved.org

Cyber-Security Information Sharing Partnership
www.cisp.org.uk

Cyber Security Strategy 2011
www.gov.uk/government/publications/cyber-security-strategy

Department for Business, Innovation and Skills
www.gov.uk/government/organisations/department-for-business-innovation-skills

Electronics and Computer Science Department, University of Southampton
www.ecs.soton.ac.uk/research/overview

The Foundation for Science and Technology
www.foundation.org.uk

Higher Education Funding Council for England (HEFCE)
www.hefce.ac.uk

Home Office
www.gov.uk/government/organisations/home-office

Information Security Group, Department of Computer Science, UCL
http://sec.cs.ucl.ac.uk/

Jisc
www.jisc.ac.uk

Research Councils UK
www.rcuk.ac.uk

The Royal Academy of Engineering
www.raeng.org.uk

The Royal Society
www.royalsociety.org

Security Group, Computer Laboratory, University of Cambridge
www.cl.cam.ac.uk/research/security/

The Foundation for Science and Technology
A Company Limited by Guarantee

Registered in England No: 1327814
Registered Charity No: 274727