HOUSES OF PARLIAMENT
PARLIAMENTARY OFFICE OF SCIENCE & TECHNOLOGY

POSTNOTE

Number 389 September 2011

Cyber Security in the UK

Cyber security refers to defences against electronic attacks launched via computer systems. This POSTnote looks at approaches to cyber security in the context of large-scale attacks, with a focus on national infrastructure.

Overview

- Cyber security was one of four top priorities for UK national security in the 2010 National Security Strategy.
- Effective approaches to cyber security integrate technological measures with those relating to processes and personnel.
- There is no overarching regulation of cyber security in the UK, although a growing number of organisations are complying with voluntary standards.
- Better communication of cyber issues and solutions within industry, and between industry and government, is needed to strengthen overall resilience and security.

Background

The term cyber attack can refer to anything from small-scale email scams through to sophisticated large-scale attacks with diverse political and economic motives. Large-scale attacks may have a number of interrelated aims such as:

- gaining unauthorised access to sensitive information;
- causing disruption to IT infrastructure;
- causing physical disruption (e.g. to industrial systems).

The recent "Stuxnet" attack has heightened debate on cyber security in the context of national infrastructure (NI).[1] NI is defined as "facilities, systems, sites and networks necessary for the functioning of the country and delivery of the essential services upon which daily life in the UK depends".[2] Such infrastructure increasingly has both physical and IT components. Cyber attacks have not caused physical disruption in the UK to date, although they have disrupted IT systems. More common types of attack, such as cyber fraud and intellectual property theft that are estimated to cost the UK £27 billion a year,[3] are not the focus of this POSTnote.

Governance

The first UK Cyber Security Strategy (**CSS**) was produced by the previous government in June 2009. It stressed the need for "a coherent approach to cyber security", with the government, industry, the public and international partners sharing responsibility. Following the CSS, two new bodies were formed with responsibility for developing a coordinated approach to tackling cyber security (Box 1). Following the 2010 National Security Strategy, the Strategic Defence and Security Review allocated £650 million of additional funding to the new National Cyber Security Programme (**NCSP**) over four years. The government is due to produce a new CSS in October 2011. This will outline the government's position on the role of the private sector in tackling cyber security, which is crucial given that around 80% of the UK's critical national infrastructure is privately operated. It will also outline funding allocations through the NCSP, of which some detail has already been communicated.[4]

Box 1. Responsibility for UK Cyber Security

- The Office of Cyber Security was formed in 2009 and became the Office of Cyber Security and Information Assurance (OCSIA) in 2010. OCSIA is located in the Cabinet Office and coordinates cyber security programmes run by the UK government including allocation of the National Cyber Security Programme funding.
- The Cyber Security Operations Centre (CSOC) was formed in 2009. CSOC is housed with GCHQ and is responsible for providing analysis and overarching situational awareness of cyber threats.
- The Centre for the Protection of National Infrastructure (CPNI) provides guidance to national infrastructure organisations and businesses on protective security measures, including cyber.
- CESG is the National Technical Authority for Information Assurance and is situated within GCHQ. CESG provides information security advice and a variety of information assurance services to government, defence and key infrastructure clients.
- Computer emergency response teams (CERTs) exist in a number of public and private sector organisations. GovCERTUK is responsible for all government networks, while CSIRTUK, CPNI's CERT, responds to reported incidents concerning private sector networks in the critical national infrastructure.

A recent inquiry by the House of Commons Science and Technology Committee recommended that the "government clarify the powers and funding" of OCSIA.[5] It is hoped that

the second CSS will resolve this issue. Some changes have been made since the inquiry closed. For instance in May 2011 ministerial responsibility for cyber security was moved to the Cabinet Office.[4]

Types of Large-Scale Cyber Attacks

Data Theft and Cyber Espionage

Cyber attacks have aimed to steal sensitive information and data from financial, government and utilities infrastructure targets (Box 2). These attacks can target intellectual property or sensitive information about organisations or government. Many data theft attacks succeed because of lapses in security practice on the part of personnel, such as succumbing to email scams. Data theft attacks may provide information that could facilitate further high profile attacks.

Attacks on Information Infrastructure

Critical information infrastructure (CII) may refer to any IT systems which support key assets and services within the national infrastructure. Understanding of the vulnerabilities of CII is still evolving. The chances of an attack undermining the operation of the internet as a whole are considered low, as the internet has a high level of inherent resilience. For example in the event of a loss of service in one geographic location, data could simply be rerouted, avoiding impacts over a large area. The lack of any successful attacks of this nature to date and the fact that much relevant information is not in the public domain, mean that it is hard to speculate about the level of risk. Nevertheless, in principle, there are scenarios that could lead to widespread disruption of internet services. Some signs of attempts to undermine the operation of such fundamental CII have been observed, although to date none has been successful. Successful, targeted, attacks have been conducted against individual CII services and have caused short term damage. However, these are difficult to sustain, particularly when targeting well protected critical information assets (Box 2).

Attacks on Physical Infrastructure

Utilities infrastructure and industry increasingly rely on computer systems and networks. Cyber attacks on these systems therefore have the potential to cause physical disruption. One way is through targeting a specific type of system called supervisory control and data acquisition or **SCADA** (Box 2). These systems are found throughout industry as well as in water, electricity, gas and transport infrastructure. They collect data from sensors; these data are then used to inform commands sent to computer-operated devices that control industrial processes.

SCADA systems have requirements which mean that standard security techniques cannot always be applied. While systems are in operation (for example, if a power plant is online) it may not be safe to carry out significant updates and security tests on them. Some security experts comment that reliance on SCADA systems means that physical industry and infrastructure are vulnerable to attack. However, there are many obstacles to SCADA-specific attacks. Historically, SCADA systems have been based on highly specialised software and hardware. While industrial systems use generic SCADA components, they will be configured to specific industrial processes. Thus a cyber attack on SCADA would be likely to require sophisticated and in depth knowledge of the target as well as considerable skills and resources. Security firm Symantec estimate Stuxnet took 5-10 people six months to program (not including the resources needed for espionage) and that the code was possibly tested on a physical replica of the target facility.[7] However it is possible that less sophisticated attacks could still cause disruption (see Page 4).

Box 2. Examples of High Profile Cyber Attacks

Data Theft: RSA Security, Lockheed Martin and the IMF
There have been numerous cases of data theft from large organisations in 2010 and 2011. An attack on the security firm RSA in 2011 led to user authentication technology being stolen. This, in turn, led to hackers gaining access to defence contractor Lockheed Martin, although officials stated no sensitive data were obtained. The International Monetary Fund announced in June 2011 that a cyber attack against its systems had been successful, although the IMF have not disclosed whether sensitive data were stolen.

Information Infrastructure: Estonia, SOCA, CIA
There have been a number of distributed denial of service (DDoS – see Box 3) attacks on information infrastructure over the last five years. In 2007 DDoS attacks targeted Estonian banking, police and government websites. Estonian information infrastructure was poorly prepared to handle the attack.[6] To tackle the attacks, access to Estonian hosted websites was denied to users outside the country. In 2011, hacking groups targeted DDoS attacks on UK and international public sector and governance internet services, including the Serious Organised Crime Agency and the CIA. In both cases the attacks were effective for less than a few hours, affecting public information websites rather than compromising any critical data or systems.

Attacks on Physical Infrastructure: Stuxnet[7]
Discovered in 2010, *Stuxnet* was a piece of sophisticated malicious software that targeted industrial systems produced by Siemens. It is thought that the attack aimed to impede the operation of centrifuges used by the nuclear industry in Iran to separate isotopes of uranium. Although a reduction in the number of operational centrifuges in Iran in 2009-10 was observed, there appears to have been no lasting impact on capacity.[8] As of March 2011, Siemens were aware of 24 clients with industrial systems infected by Stuxnet (out of thousands of Siemens systems installed globally). No adverse effects have been observed in these infected systems, as Stuxnet was only designed to affect very specific targets. Around 100,000 Windows-based computers worldwide have been infected according to Symantec.

Tackling Cyber Security

Protecting against cyber attacks requires action at many levels. Implementing technological solutions is vital but the skills, behaviour and attitudes of personnel are equally crucial. The organisational processes to manage these information risks are collectively known as information assurance (IA). Rather than focussing on specific attack examples when designing security measures, it is considered best practice to use a holistic approach employing a combination of solutions to address a wide range of possible vulnerabilities.

How Cyber Attacks Are Carried Out

Attacks on computer systems can be launched through the internet and can also be carried out against isolated systems, for example via USB devices. Large-scale attacks often require sophisticated engineering, where malicious

software is tailored to suit the target, although untargeted attacks can also infect and disrupt critical systems. Regardless of the various methods to reach a target (Box 3), most large-scale attacks must exploit both:

- Technology: technological flaws can be exploited to gain access to or privilege within a computer system. For example, software vulnerabilities can be exploited to gain administrator control. Vulnerabilities can often be due to the software not being up to date. In rare cases hackers exploit previously unknown (and therefore unprotected) software flaws, so called **zero-day** attacks.
- People: cyber attacks exploit vulnerabilities in human behaviour, including lack of awareness of security practices. This is often referred to as "social engineering". For example, employees may be led into downloading malicious software or using an infected USB drive. Insiders may attempt to use their authorised access to systems for unauthorised purposes.

Box 3. Types of Cyber Attacks

Cyber attacks can be launched by hackers themselves or from computers that have been compromised to serve the hacker's need without the users knowledge (**bots**). Networks of bots (**botnets**) can act together to achieve a collective aim. Types of attack include:

- **phishing**: email scams that attempt to obtain personal data;
- **malware**: catch-all term for software with malicious intent;
- **trojans**: typically email or browser based attacks. Must be accepted by the target to launch malware on their computer. Aims include data theft and botnet recruitment;
- **worms**: a subset of malware able to spread and replicate across a network or through removable media;
- **root-kit**: software to gain and maintain privileged access to computer systems; can be used to conceal other malware;
- **distributed denial of service** (**DDoS**): floods of internet traffic from distributed sources often caused by botnets, which result in network facilities becoming overloaded and inoperable.

Vulnerability to low-level attacks such as phishing can compromise information that can then be used in large scale attacks.

Technological Solutions

A range of technological solutions exist (Box 4). Practices vary widely; over 50% of respondents in a recent survey of security specialists from a range of industries said there was a "case for improving their cyber defences".[9]

Box 4. Common Technological Cyber Security Solutions

Commonly used cyber security measures include methods that apply to both computer software security and computer network security:

- deployment of **firewalls** (devices that restrict data transmission/reception as specified by an administrator);
- use of up-to-date **anti-virus** software;
- regular **software patching** (i.e. updating; software revisions are often made to address security issues);
- **access management** systems, for example login systems using cryptographic tokens or biometric data;
- **encryption** of data communications and sensitive data;
- **intrusion detection**, for example intelligent monitoring of data traffic passing in and out of a network.

More advanced techniques exist to strengthen cyber security.

- Vulnerabilities are commonly introduced into software due to poor programming practice. By developing software carefully, and continuously assessing for vulnerabilities, **secure by design** software development increases product security. An example of this practice is Microsoft's Security Development Lifecycle.[10] A similar approach can be applied to network development, with network security being considered at the design stage.
- **Reverse engineering** involves deconstructing software to understand how it works. This is used to develop defence mechanisms against malware, but is also used to locate vulnerabilities that malware can then exploit.
- **Air-gapping** (total isolation of the network) can provide total security to attacks launched over the internet; this does not protect against attacks from within an organisation or attacks transmitted via removable media. Air gapping is increasingly rare (see Page 4).

People

Cyber security awareness and training among personnel is vital for any procedural or technological security to be effective. Failure to achieve a robust security culture is often seen as a weak link in organisations' security. The government's GetSafeOnline scheme, aimed at small enterprises and the general population, provides advice ranging from security against email scams to network protection. In addition, approximately £6.5 million of NCSP funding has been assigned to education.[11]

Processes

Organisational practices to manage both technological and personnel-related risks include:

- conducting **risk assessments** and implementing risk management. This is encouraged by government and security consultants, though the latter warn against a 'check-box' approach to risk management that constrains the range of risks considered;
- use of **penetration tests**, whereby security consultants attempt to identify vulnerabilities within an organisation's systems. These can assess technological security, IA and resilience to social engineering, providing a valuable assessment of security. However, they can be rendered invalid by subsequent changes to systems or practices;
- compliance with certifiable international **standards,** such as general information security management (ISO/IEC 27001) and specific industrial control system security (ISA-99). Such standards are regarded as a good, although generic, baseline from which to build security.

Effective emergency response procedures for handling an attack at organisational as well as national and international level are also vital.[5,12] Some national infrastructure operators have incidence response units, for example the National Grid Cyber Response Team.

Emerging Issues

Governance

Regulation

Within the public sector, IT systems must have their security verified before they can be used for sensitive purposes. A number of schemes that provide this assurance are run by CESG. These schemes are also widely recognised by the private sector, but they are not mandatory as there are no regulations on cyber security (except if this forms part of

existing regulation for specific sectors). CPNI provides guidance and advice to national infrastructure operators, and industry-wide standards are increasingly recognised. Opinion is divided as to whether cyber security regulation by government would be the most effective way forwards. Regulation could increase levels of adherence to best practice, however it will always lag behind developments in technology and would be difficult to monitor.

Communication

As technology evolves at a rapid pace, government and industry recognise the need for communication of emerging knowledge about vulnerabilities and attack methods. CPNI runs a number of information exchanges (**IE**s) for infrastructure operators, to facilitate communication. Some organisations are concerned about the limited reach and access to this communication, particularly for smaller operators, although there is consensus that CPNI has good relations with private sector operators within the critical national infrastructure. CPNI's perspective is that communications need to be conducted on a confidential basis in order to maintain mutual trust. The government is assisting industry in developing and establishing cross-sector IEs from which sector-specific hubs will disseminate information. Consultation on establishing these IEs is being led by the OCSIA; it is thought that the scheme will be operational by the end of 2012.

International Cooperation

Cyber security is a global issue. The UK is involved in international initiatives within the EU, UN and with the US and other nations. A 2009 EU communication on protection from large scale cyber attacks emphasised the role of the European Network and Information Security Agency (ENISA).[13] However, a recent ENISA-run exercise involving all EU member states found there was a lack of procedure to handle cyber incidents on a pan-European level.[14]

Industrial Control Systems

Impact of Networking and Use of Commercial Software

In the past, the cyber security of industrial control systems (**ICS**) was ensured by air-gapping the systems. SCADA devices (which can have lifetimes of decades) were not conceived to be connected to extended networks. However, there is an increasing trend to connect SCADA devices to wider networks.[15] In the water industry, for example, approximately one third of companies are upgrading SCADA infrastructure to allow control of remote sites from a central location. Future smart grid infrastructure, which will provide more control over distribution of gas and electricity (POSTnote 372), will also require a significant increase in the use of ICT infrastructure for monitoring and control. Smart grid security consultation is in its early stages, with a cyber security framework currently being developed.[16]

Legacy SCADA systems run custom-designed operating systems and software, while modern SCADA run commercial operating systems and software and communicate using internet protocol. This results in vulnerabilities to common malware through which SCADA attacks may be launched, as was the case in Stuxnet. Further to these specific attacks, infection by common malware that degrades general computer system performance could lead to significant disruption.

Responses to Emerging Cyber Security Risks

Networked SCADA systems can be protected by careful application of the cyber security options already discussed. Reverse engineering of SCADA technology has revealed vulnerabilities that allow hackers full control over specific SCADA products.[17] The US based ICS-CERT communicates when vulnerabilities are discovered in specific devices through its Control Systems Advisories. Security patches are communicated to clients by SCADA manufacturers and technological vulnerabilities are not publically disclosed unless they have been addressed. There are international examples of regulation on ICS security, for example cyber security standards for electricity infrastructure in the USA.[18] CPNI provide infrastructure operators with guidance on protective security, and coordinate an information exchange group on SCADA and Control Systems security. However, ICS manufacturers suggest that some infrastructure operators may lack the expertise in secure implementation of ICS and therefore need direct assistance in addition to guidance.

Smart Metering

Future smart metering infrastructure will provide suppliers and users with more control over gas and electricity consumption (POSTnote 301). Industry representatives argue that the only way to develop security mechanisms is through pilot schemes and by learning from the experiences of other countries where smart infrastructure is already operating. Security of smart metering is recognised as a priority by DECC and Ofgem. In response to concerns over the security of such infrastructure, DECC is working with industry to develop security requirements and specifications for smart metering systems. This is being conducted through the smart metering Security Technical Expert Group, whose members include CESG, CPNI and private stakeholders.[19] The mass rollout of smart meters in the UK (by 2019) will be based on smart meters that meet these security requirements.

Endnotes

1 POSTnote 362, 2010, Resilience of UK Infrastructure
2 Cabinet Office, 2010, Sector Resilience Plans for Critical National Infrastructure
3 Detica (report for Cabinet Office), 2011, The Cost of Cyber Crime
4 Intelligence and Security Committee, 2011, Annual Report 2010-2011
5 House of Commons Science and Technology Committee, 2011, Scientific Advice and Evidence in Emergencies
6 Institute of Electrical and Electronics Engineers Security & Privacy, 2007, The New Front Line: Estonia Under Assault
7 Symantec, 2011, W32.Stuxnet Dossier
8 International Atomic Energy Agency, 2011, Implementation of the NPT Safeguards Agreement in the Islamic Republic of Iran
9 BAE Detica, 2010, Business and the Cyber Threat: Unknowingly Under Siege?
10 Microsoft, 2010, Simplified Implementation of the Microsoft SDL
11 Ian McGhie, 2011, Speech to the Counter Terrorism Expo
12 OECD, 2010, Reducing Systemic Cybersecurity Risk
13 EU, 2009, Protecting Europe from Large-Scale Cyber Attacks
14 ENISA, 2011, Cyber Europe 2010 – Evaluation Report
15 CPNI, 2011, Cyber Security Assessments of Industrial Control Systems
16 Energy Networks Association, 2011, UK Smart Grid Cyber Security
17 NSS Labs, 2011, Analysis Brief: Siemens PLC Vulnerabilities
18 North American Electric Reliability Corporation, 2009-2011, CIP-002 – CIP-009
19 Ofgem & DECC, 2011, Smart Metering Implementation Programme

POST is grateful to Matthew Mottram for researching this briefing, to the Science and Technology Facilities Council for funding his fellowship, and to all contributors and reviewers. For further information on this subject, please contact the co-author, Dr Chandrika Nath.