Critical infrastructure protection

Dr Andrew Jones, Head of Security Technology Research, BT Security Research Centre, Adjunct, Edith Cowan University

Andy Jones looks at different approaches to critical infrastructure protection in different parts of the globe.

"Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. These systems are so vital, that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."
- President William J. Clinton, 1998

The concept of the Critical (National) Infrastructure came into public view around the middle of the last decade of the 20th century, when the US started to acknowledge that it had identified that there were a set of facilities and services that came together to provide the elements that were 'critical' to the running of a country and the well being of its citizens. The types of organizations that were included in the lists of those facilities and services varies from time to time and from report to report, but there is largely agreement that power, water, fuel supply, communications, the transport system, the finance sector, government and Public Services will be included as 'critical' elements of the infrastructure.

Paranoid

The point at which people start to get paranoid about the issue of critical infrastructures is when they assume that all of these elements will be essential all of the time. The reality is that we are used to, and can deal with, the failure of individual systems as long as they are available to most of the people for most of the time (and some of them at specific times). There is a point at which the failure of one or more of them becomes a threat to the good governance of a nation and the well being of the populace. A loss of power for four hours in the city of London might be an inconvenience but an extended loss of power for 48 hours would cause mayhem, impacting finance and trading markets, knocking out transport in the centre of London and affecting communications as Uninterrupted Power Supply (UPS) systems fail and generators run out of fuel.

UK

In the UK it took a couple of years more and the Government Committee to convince us that we had a similar problem as the US as we also had a critical infrastructure that needed to be protected in a way that was different to the measures taken in the past.

Services and facilities that are critical to the government and the people are not new. During times of civil unrest and wars, it has long been recognized that it is essential to protect things such as food and water supplies. When the ruling classes lived in castles, they recognized that in order to survive, they needed to gather the crops in, bring the herds inside the castle walls and protect the wells to ensure the supply of potable water if they were to be able to survive a siege.

Physical installations

In more recent times, the police and the armed forces have been used to protect physical installations such as the ports, power plants, railway stations, goods yards and airports. This was a suitable response to the perceived threats to those services and facilities. This is a well established process that provides increased protection to those physical assets that are considered important. What changed in the late 20th Century was largely driven by advances in technology and in particular, the Internet, when people started to realise that this protection was not enough. With the increased dependence on this connectivity that was taking place it became apparent that it was now possible for an attack to take place without an attacker ever visiting the target.

Interconnectivity

The new technologies that became available during the last quarter of the 20th Century provided the opportunity for organizations to increase efficiency and to reduce their cost of operations through changes such as centralised management processes and reduced stock holdings from just in time processes. In order for these benefits to be viable, there was a need to use the technologies so that, over time, electronic processes replaced human supervision/intervention and mechanical processes. At first, the human/mechanical ability was retained as a fallback, but over time, this became impractical to the point where, today, except in the most sensitive of systems, it is either impractical or just not possible. Another requirement that had to be satisfied in order to gain the benefits of the new technologies was the interconnection of what had previously been separate systems to allow for the automation of processes. If you want to move to a 'just in time' stock process, the organization needs to connect systems such as stock control, electronic point of sale (EPOS) together with those of its suppliers so that when an item is sold, the stock holding is automatically updated and when the threshold level is reached, an automatic order is issued to the supplier. Imagine the damage that someone with malicious intent could achieve by changing any of the barcodes on the

What happens when the lights go off? The level of CNI interdependence is often complex and not fully understood.

items, or the stock holding database or the restock thresholds or just the simple obstruction of the interchange of accurate timely information.

While this may seem a trivial example, consider how this might apply to elements of the Critical National Infrastructure (CNI). Imagine all of the major supermarkets running out of the essentials because of tampering, or even worse, the public panic buying because they had heard rumours of such a likelihood. Across the whole of the CNI there is a level of interconnectivity and interdependence that is becoming increasingly complex and that in some cases is not fully understood.

No power

An example of a large scale failure of an element of the CNI can be seen in the incident in August 2003 when more than 50 million people in eight states on the east coast of the US and one Canadian Province were left without power. The fault was blamed on failure of three power lines in Ohio State according to some reports while others said it was the result of a tree falling on power lines near Cleveland. It is an indication of the fragility of the systems that we rely on that such trivial single incidents could have such dramatic effects. The power loss affected some of the people for up to four days but whilst not creating a major crisis did have significant economic impact. The financial market had to invoke fallback capabilities and several organizations moved their centres of operational control out of the affected areas. In all probability there were cases of lost lives but they were masked by normal daily occurrences of such incidents.

An analysis of the incident showed that this failure was the result of an accident, but the potential for a similar major event that was initiated as a result of a malicious act is obvious. If an accidental failure can have this level of impact, it is not difficult to imagine what could be achieved if there was a purpose to it. What was interesting in this and a number of other similar incidents which took place around two years after 9/11 was that after early investigations and rebuttals of suspicions that they may have been terrorist incidents, there was a notable lack of panic amongst the population, despite the widespread effects of the incidents.

In the UK, the Government has defined the CNI as consisting of those assets, services and systems that support the economic, political and social life of the country that are of such importance that any full or partial loss of them could cause:

- Large scale loss of life.
- Have a serious impact on the economy of the UK.
- Have other grave social consequences or be of immediate concern to the government.

There are many views on what elements come together to form the critical national infrastructure. In the UK, the National Infrastructure Security Coordination Centre (NISCC) has identified what it believes are 10 main interdependent sectors, which they list as:

- Communications.
- Emergency services.
- Energy production and distribution.
- Finance.
- Food.
- Government and public service.
- Health.
- Public safety.
- Transport and water.

Independent ownership

One of the main problems with protecting the critical national infrastructure that exists is that many of the elements of the CNI are owned by a range of independent, mostly commercial, organizations. While each of these individual organizations take security measures to protect their individual interests and those of their shareholders, it would be unreasonable to expect that they would invest in measures to secure those aspects that are of relevance to the nation state.

One of the issues that has most exercised the minds of those in respective governments is how to interact with the organizations that own and control the critical infrastructure. In the UK, there are a large number of individual power generation and supply, water, transport and financial organizations, many of them owned by companies that are headquartered in other countries. Most of them are also

public companies and have to answer to shareholders to make the best return on their investment that is possible.

It may seem strange that, even in the western world, there have been a range of different approaches taken to the protection of the CNI. The USA, the UK and most of Europe have adopted similar models for addressing the problem. This is understandable as each of these regions have realised that the protection of any national infrastructure cannot be fully addressed by any one nation state and that there is a need for international collaboration and communication.

Interestingly, Sweden has taken a totally different approach. This is an indication that, despite CNI protection being a global problem, with the potential to benefit from knowledge and information that is created elsewhere; it is possible for different regions and cultures to approach the problem in different ways. While considerable effort has gone into testing and evaluating the processes and procedures that have been implemented to protect the CNIs under both approaches, it is also true that those that would seek to cause harm are also constantly developing new ways to do so. Hopefully we will never be in a position to be able to compare how effective the different approaches have been.

Europe

In Europe, which has no direct control over the protection of the infrastructures of independent member states, the approach that has been taken to address the problems that are envisaged in protecting the collective CNIs have included the creation of the European Network and Information Security Agency (ENISA)[1] and the development of the European Network for Critical Infrastructure Protection (EPCIP) and the Critical Infrastructure Warning Information Network (CIWIN). All of these efforts have been designed to assist and support the individual national efforts.

UK

What has the government done? In the UK one of the major developments that the Government undertook in 1999 was the creation of the NISCC. This organization is a multi-agency group that calls on the expertise and efforts of a range of government agencies including Central Government, Defence, Trade and Industry, the Intelligence Agencies and Law Enforcement. The organization was created with the primary role of minimising the risk to the CNI from electronic attack. Another development was the creation of the Cabinet Crisis Committee, which was created as a result of the fuel strike in the UK that took place in September 2000 when the government was taken by surprise by the effect that a small number of protesters, with very little planning and organization, could have on the infrastructure.

NISCC

The NISCC has attempted to fulfil its role through a number of areas of work that include the production of Threat Assessments, an initiative to warn organizations of new threats and ways in which their effects can be minimised or mitigated, assistance in the investigation of incidents and recovery, an outreach programme to encourage information sharing and to offer advice and foster best practice and also the support of relevant research and development. One of the issues that NISCC believes that it can and must address is the issue of the transnational nature of the problem. On 1 February 2007, as part of government reorganization, NISCC merged with NSAC (National Security Advice Centre) and will, in future, be know as the Centre for the Protection of National Infrastructure (CPNI). One good thing that has come about from the transition to the new structure is that they have learned the lessons from the reorganization of the police under the Serious Organised Crime Agency (SOCA). This reorganization left the public with the perception that the National High Tech Crime Unit (NHTCU) had totally disappeared into SOCA and left no apparent point of contact or access to the resources that had previously been available. I am happy to say that the CPNI website was immediately available and has provided a continuity of advice from central government.

US

In the US, the government approach has evolved over time and is now led by the Department of Homeland security. In 1998 the President signed Presidential Decision Directive 63 (PDD 63) and in January 2000, President Clinton announced the 'National Plan for Information Systems Protection'. One of the very successful US initiatives for CNI protection is InfraGard. This is a Federal Bureau of Investigation (FBI) programme that was established in 1996. It was started as a local attempt to gain support from the information technology industry and academia for the FBI's investigations in the high tech area. This was then expanded to what was, at that time, the National Infrastructure Protection Center (NIPC) and then, subsequently to the Cyber Division in 2003. The purpose of the InfraGard programme has been to develop a trust relationship and provide some credibility in the exchange of information regarding a range of matters including crime, terrorism, intelligence and security. As part of the InfraGard Programme a number of Special Interest Groups (SIGs) have been created to address the issues related to the safeguarding of specific critical infrastructures in both private industry and the government through information-sharing networks. The overall aim of the InfraGard programme is to improve the sharing of information between private industry and the government on critical national infrastructures.

Swedish alternative

The Swedish approach to Critical Infrastructure Protection (CIP) varied from that which prevailed in most

of the rest of Europe and the US. In Sweden, in 2002, they created a central authority, the Swedish Emergency Management Agency (SEMA), to address any type of crisis that might be encountered. The Agency is structured in such a way that, when strategy and a course of action have been decided, orders can be distributed to the relevant administrative and information departments. From there, orders can be given to the relevant areas of research, planning, emergency, International CIP management, public safety radio, technical, and information assurance and analysis departments. While this is a centralised system, it has been developed in a way that is considered to be supportive of the individual areas.

One of the major problems that the UK elements of the Critical National Infrastructure dealt with was trying to identify and understand the threats that their businesses face. The Government had, historically, produced threat assessments for the UK as a whole, if you like, 'UK Plc,' but they had not been required to consider or produce threat assessments for individual business sectors. There was an additional problem with how any threat assessments they produced for an element of the CNI could be disseminated to the relevant businesses in a way that was fair and accurate and which could be released to organizations under overseas ownership. While the experience that existed within government was for the production of national threat assessments, the generation of assessments that related to specific elements of the CNI was a new concept and called for a new set of skills and knowledge. These skills have taken time to acquire; as has the development of the relationships with the various sectors of the infrastructure, but there has been good progress during the last few years.

How might an attack on the CNI manifest itself? The attacks of 9/11 and 7/7 were clearly attacks on the national infrastructure, but both were attacks against the physical rather than the electronic infrastructure. However, we have also seen warnings that have been issued by NISCC about a long standing and ongoing attack on all areas of the UK national infrastructure from the Far East. While NISCC did not specify which country, the US was a little more forthcoming and accused China of undertaking the attacks. These attacks have apparently focused on the collection of intelligence from Western organizations rather than an attack to disable elements of the CNI. Considerable experience has now been gained with major incidents of power failure, terrorist alerts that have had a major impact on ground and air transport systems and the fuel strikes. From this, it is clear that a major attack on the infrastructure, whether an attack on the physical or the electronic infrastructure, could have a significant effect in the short term. However, in the longer term, the indications are that the relevant authorities and the majority of the population will adapt and make do until the previous status quo is restored.

One scenario that was postulated by Winn Schwartau in his 2002 novel *pearl harbor dot com* was of a CNI attack on the computers of the financial sector in the US. While this was only one scenario that was put forward by an early evangelist of the vulnerability of information systems, it did capture the essence of the effects of the 9/11 attacks on the confidence of the populace on the underlying infrastructure.

Why aren't we winning? Well, the first question that we should ask is 'who says we are not?' We are very good at publicising the weaknesses and failures, but are much more conservative about shouting about the successes. Perhaps this is partially the British conservatism and partially the legacy of the organizations that came together to form the NISCC – the security service, Government Communications Headquarters and the Department of Trade and Industry – the first two with a history of keeping secrets secret and not renowned for their communication links with industry. As NISCC matured, it was clear that considerable effort was being put into ensuring that appropriate information was being pushed out into the public domain and, over time, this was increasingly well balanced.

Conclusions

There has clearly been a huge investment by governments around the world to understand and to protect their individual critical infrastructures and there has been significant international collaboration to share knowledge and, in some cases, resources. The two major issues that they have encountered are that, for the most part, the governments do not own the elements that come together to form their critical infrastructures and the immense complexity of the interdependencies of those infrastructures.

This would have been a difficult enough problem had the businesses and technologies that the CNIs are made up of been static, but in reality, in the decade or so since we first appreciated that there were such structures, there has been significant changes in dependence, structure, process and technology in some of the sectors. There have been a large number of mergers and acquisitions, convergence of business in the areas of telecommunications, information technology and broadcasting and a significant change in the technologies that are used.

The protection of the elements of the critical infrastructures will ultimately remain the responsibility of the organizations that own them, as they are the only ones that have the knowledge and access to protect them. Governments are likely to continue to support these efforts with information on threats and advice as well as regulation of the sector. They will also be able to take steps such as those taken by the US which has just increased

its strategic holding of oil to counter OPEC control of the market sector. Governments may also be able to provide limited resources in the event of an attack, but are unlikely to provide the level of funding that would be required to improve the security and survivability of most of the elements to a level that would make a significant difference. The area where it would appear that governments can have the most significant impact will continue to be the provision of timely advice and the early investigation of incidents to determine the likely cause in order to prevent unnecessary panic or overreaction.

About the author

During a full military career Andy Jones directed both Intelligence and Security operations and briefed the results at the highest level and was awarded the MBE for his service in Northern Ireland. After 25 years of service with the British Army's Intelligence Corps he became a business manager and a researcher and analyst in the area of Information Warfare and computer crime at a defence research establishment. In September 2002, on completion of a paper on a method for the metrication of the threats to information systems, he left the position to take up a post as a principal lecturer at the University of Glamorgan in the subjects of Network Security and Computer Crime and as a researcher on the Threats to Information Systems and Computer Forensics. At the university he developed and managed a well equipped Computer Forensics Laboratory. He holds a Ph.D. in the area of threats to information systems. In January 2005 he joined the Security Research Centre at BT to take up a post as a research group leader.

[1] ENISA web site on Risk Management has been recently released. This web site contains material from the area of Risk Management and has now been expanded with information from the thematic area of Emerging Risks. This material is available from the ENISA Risk Management URL: http://enisa.europa.eu/rmra

Governance and security: side by side

Piers Wilson, Head of Technical Assurance

Piers Wilson

It seems like everybody is talking about governance these days, certainly large multi-national organizations, with high profiles, powerful shareholders and complex financial affairs. Financial and other sector regulators are also establishing "good governance" as a business holy grail that essentially all companies must aspire to. Product vendors have taken this on board as it is seen as the latest easy way to sell products; IT managers have tired of promises of reducing Total Cost of Ownership (TCO) that didn't really deliver, solutions that would "e"-enable their business, automate their supply chain, etc. Pitching your product as some sort of solution to achieving governance not only sounds great, but it might just get the attention of board members who, slightly scared by the degree of regulation, might just make a snap purchase decision if they think it will somehow help.

The thing about corporate governance…

On a basic level, Corporate Governance is about managing anything which could undermine the trust in, or give rise to risks to, the organization. As such it encompasses the processes, policies and laws affecting the way an organization/corporation is managed, administered or controlled. A key concept of this is corporate accountability and trust, which means having processes and mechanisms in place to ensure responsible behaviour and the protection of shareholders. These might include:

- Effectiveness and efficiency of operations.
- Reliability of financial reporting.
- Compliance with all laws and applicable regulations.
- Safeguarding of corporate assets, including physical and information.

The Organization for Economic Cooperation and Development (OECD) principles of Corporate Governance requires timely and accurate disclosure of material information on "foreseeable risk factors" and corporate policy and the process by which it is implemented.

It is hard to see how these days, one could claim that the myriad of IT security risks such as viruses, hacking, misuse by staff, phishing, denial-of-service, active code etc. are not "foreseeable risks."

Corporate Governance is though (of course) much bigger than just IT/information security.

The thing about security…

Security of course, is also about managing "foreseeable risks" and having policies and controls in place. In many respects some aspects of the work I do particularly around penetration testing, is to try and find what risks exist and how systems might be attacked (then advise on how to defend systems against those risks).

What security and governance do have in common though is the concept of trust - in an organization, its practices, data safeguards, and operations rely not only on sound