Roinn Cumarsáide,
Fuinnimh & Acmhainní Nádúrtha
Department of Communications,
Energy & Natural Resources

National Cyber Security Strategy 2015-2017

Table of Contents

Executive Summary

The National Cyber Security Strategy (2015-2017) sets out how Ireland will engage with a dynamic and challenging aspect of developments in digital technology, setting out the Government's approach to facilitating the resilient, safe and secure operation of computer networks and associated infrastructure used by Irish citizens and businesses. The development and proliferation of Information and Communications Technology (ICTs) has resulted in dramatic improvements in quality of life, the delivery of new and innovative services, and sweeping changes in the way in which businesses operate. However the growing use of these technologies has resulted in society becoming, to a degree, dependent on the ongoing operation and resilience of these systems. A range of threats have emerged to the safe and secure operation of ICT networks, emanating from a diverse set of sources. These threats can be loosely categorised as hacking, cyber-crime, hacktivism and cyber espionage. Equally, reliance on these networks and systems has led to risks engendered by human error, software and equipment failures and even extreme weather events. This document engages with these various threats and hazards, sets out the high level strategic goals that form the basis of national policy in this area and establishes the measures that will be taken in respect of each.

In particular, the Strategy includes the establishment of the National Cyber Security Centre within the Department of Communications, Energy and Natural Resources, and details how that body will engage with its three primary areas of responsibility; government networks, personal and business systems, and the protection of critical national infrastructure. This will build on the existing Computer Security Incident Response Team (CSIRT-IE), established in late 2011.

1. Introduction

1.1 Background

The National Cyber Security Strategy (2015-2017) sets out how Ireland will engage with a dynamic and challenging aspect of developments in digital technology. The use of internet technologies and ICT more generally to enable government, business and individuals to deliver, participate and inform themselves has been transformative, but has also opened up vectors for new types of attack. The fact that the digital domain encompasses all information infrastructures accessible via the Internet (or otherwise), and transcends territorial boundaries makes this arena far more complex and potentially dangerous than would otherwise be the case.

In 2013 the World Economic Forum identified cyber-related threats as one of the highest of all global risks from both the perspective of impact and likelihood[1], a finding mirrored at a national level in the 2014 National Risk Assessment[2]. The State, critical infrastructure, businesses and citizens depend upon the reliable functioning of information and communication technologies and of the Internet. Disruption to these systems, regardless of the source, poses a direct threat to the functioning of the State and the economy, and can have profound effects on the daily life of millions of citizens. The Internet is already critical to the economic and social well-being of the State. Moreover, it possesses enormous potential to make an even greater contribution to economic and social development. Any threat to its resilience and security therefore requires a robust and coherent response, both nationally and at an EU and international level.

This Strategy presents a cross-government framework for ensuring cyberspace remains safe, secure and reliable, with an emphasis on task-sharing and building trust relationships between the State, public and private partners, academia and civil society.

[1] Global Risks Report, 2013.

[2] http://www.taoiseach.gov.ie/eng/Publications/Publications_2014/National_Risk_Assessment_report_2014.pdf

As events and technology continue to evolve, flexibility will be necessary and will be reflected in an adaptive and flexible implementation of the Strategy.

2. Context - People, Economy, and State

2.1 Citizens

Cyber security is not limited to the application of technical solutions to improve the security of networks, devices or data. Rather, the nature of the challenge is such that a diverse range of measures are required, including the delivery of timely and appropriate regulatory responses by governments, inducting an ongoing process of technological adaptation and improvement and fostering a cultural understanding of the importance of the issue. Ensuring that each of these tasks are delivered is a prerequisite for open, free and safe access to cyberspace, and confidence that their personal data will be processed in accordance with data protection principles enshrined in law, notably national legislation, the European Union Treaties and the European Convention on Human Rights. The Internet is a resource to which all citizens can and should have access. As an information-led society, Irish citizens socialise, entertain, communicate, learn, transact, and to varying degrees, live, online. Protecting this lifestyle and individuals' personal data is a prerequisite for prosperity, social development and the protection of human rights.

2.2 Economy

Ireland's economy depends on effective and secure digital infrastructures for sustained growth and development. The digital economy contributes 5% of national GDP and is growing at approximately 20% annually. There are few sectors that do not rely on ICTs for their operations, including a wide range of critical economic infrastructure such as electricity, gas, financial services and water supply. Nine out of the top ten global software companies, all of the top ten global ICT companies, and the top ten "born on the Internet" companies possess significant operations in Ireland. Protecting and sustaining this investment, which provides employment for over 100,000 people, is a vital priority for Ireland. Securing the long term future of this sector is of crucial importance to the economy, and within this sector information security represents a particular growth opportunity for Ireland. There is a real potential for Ireland to become a cyber-security hub on the basis of the nascent cloud computing and big data sector developing in the State.

2.3 Risks

The diverse ways in which network connected technologies are used, together with the extremely widespread proliferation of devices, means that a very wide range of risks have already arisen, both in terms of the type of threat and in terms of origin. The type of threat ranges from relatively low level attempts to generate publicity, to extract banking or other information, through to large scale data exfiltration and even sabotage of ICT systems. In some cases, attacks have resulted in physical damage to equipment and infrastructure. The origins of such attacks range from lone individuals to criminal groups, and in some cases likely include Nation States seeking to gather intelligence or to damage or degrade infrastructure. Incidents arising through extreme weather, human error and hardware or software failure also pose significant risks to individuals, businesses and public administration.

In a great number of cases, the risks to individuals, companies and the State are similar, and can be mitigated by the application of the same responses, including good practice such as business continuity planning, keeping software up to date or ensuring that individuals are aware of risks that arise online, and trained to deal with them. In some cases however, more specific and complex threats arise, such as in those cases where businesses control large amounts of data or operate critical infrastructure; in these instances more severe risks arise and a more involved set of responses is required. On a national level, Ireland faces a more complex set of risks than many other countries. The presence of a large number of data centric international companies here, and the growing number of data centres present in the State mean that the potential for reputational damage is an important consideration.

2.4 Government

A number of initiatives have been introduced by the Irish Government which optimise and promote use of information systems for economic and social growth.

- The Government's National Broadband Plan aims to ensure that all citizens and businesses have access to reliable high speed broadband, opening up new business, economic and social opportunities.

- Ireland's National Digital Strategy "Doing More with Digital", published in June 2013, is focused on increasing the extent and quality of online engagement.

- The eGovernment Strategy 2012-2015 report (April 2012), describes a reformed public administration which is moving towards online channels for public engagement and service delivery.

- The national "Action Plan for Jobs" (2013), aims to provide sustainable employment and seeks to improve economic infrastructures, encompassing secure ICT, to make Ireland a more environmentally-friendly, safer and more pleasant place in which to live and work.

- The Public Service ICT Strategy published in January 2015 focuses on leveraging improved efficiencies from innovative use of new and emerging digital technologies for citizens and businesses.

The developing national and EU research agenda has also placed an emphasis on research, both through the Digital Agenda and the Horizon 2020 Programme (which includes a specific strand on Digital Security).

The majority of the services provided by the State rely, to some extent or other, on ICT systems. These include basic but essential email and telephony services and a wide range of databases containing the personal data of millions of citizens and the business data of companies operating in the State. These systems also include a wide range of online platform services, including those run by the likes of the Revenue Commissioners and the Department of Agriculture, which are central to the business operations of these bodies and of customers.

2.5 Critical National Infrastructure

Critical National Infrastructure (CNI) comprises essential services such as electricity, water, transportation, telecommunications, commerce and health. The convergence of networks and information systems now means that the provisioning of these services substantially relies on the seamless operation of Information and Communication Technologies. The systems, services, networks and infrastructures that underpin other

Critical Infrastructure, or provide essential services themselves, are called Critical Information Infrastructure (or CII) and include telecommunications networks, the Internet, terrestrial and satellite wireless networks.

While all infrastructure is at risk from damage or destruction by natural or manmade events, damage to either CNI and CII could have negative consequences for national security, the economy, or the well-being of citizens of the State. While measures have long been in place to ensure the security of such infrastructure against damage from conventional sources, there is a growing awareness of the risks posed to infrastructure by cyber attack. However, there is a substantive difference between the traditional realm, where kinetic attacks require a physical proximity and which are generally easily attributed, and cyber attacks, where neither of these factors are necessarily present. The growing sophistication and apparent proliferation of cyber attacks on infrastructure means that this cannot be ignored. This Strategy contains a series of measures to strengthen capacity in this area.

The extant Computer Security and Incident Response Team (CSIRT-IE) within the Department of Communications, Energy and Natural Resources have been engaged in general emergency planning processes in the State with the Principal Response Agencies (including An Garda Síochána, the Health Service Executive and the Local Authorities), Government Departments and other agencies overseen by the Office of Emergency Planning (OEP) within the Department of Defence and the Government Task Force on Emergency Planning, chaired by the Minister for Defence. This includes contributing to the development of a National Framework for Emergency and Crisis Management in Ireland, which aims to foster national resilience in the face of emergencies/crises, thus minimising or mitigating the disruption of national life and achieving the optimum outcome when an emergency occurs. The Government's Cyber Security Strategy sets out how Ireland will protect and improve the cybersecurity of Critical National Infrastructure in the context of national emergency planning.

2.6 European and International Developments

Since 2001 there have been a number of EU and international measures aimed at improving Network and Information Security. These have included the establishment of the European Network and Information Security Agency (ENISA) in 2005, the facilitation

of awareness raising events, training, cyber security exercises and the development of policy proposals and platforms such as the 2009 Communication on Critical Information Infrastructure Protection[3]. The 2010 Digital Agenda for Europe[4] included a range of actions designed to ensure greater trust and security online, including that Member States would establish "… *a well-functioning network of CERTs at national level covering all of Europe*" by the end of 2012. The EU Telecommunications Framework Directive (2009/140/EC) already provides for mandatory and security requirements for telecommunications operators. In 2013, the EU published a Cyber Security Strategy focusing on 5 key pillars; namely improving cyber resilience, addressing cyber-crime, facilitating improved cyber defence capabilities, research and industrial development initiatives for industry and diplomatic initiatives focused on developing the rule of law and norms of behaviour for States.

However, the increased threat level has led to a persistent concern that the EU was losing ground in this area, and as such the Commission published a proposed Directive in 2013. This draft Directive, termed the Network and Information Security (NIS) Directive has been the subject of intensive discussions at European Council and Parliament, and will likely be agreed later in 2015. It sets out obligations for all Member States concerning the prevention, handling of and response to cyber incidents and attacks affecting information communications technology systems in some online businesses, energy, transport, banking and financial services and health sectors. The draft Directive also has a number of specific requirements, including:

- the development of a strategy at national level;
- the designation of a national competent authority or authorities;
- the establishment and resourcing of one or more national computer security incident response teams (CSIRTs);
- the development of co-operation arrangements between Member States at strategic and operational levels; and

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

[4] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN

- the reporting of network and information security incidents and conformance with risk management and security requirements for specific undertakings providing information society services or operating critical infrastructure in the energy, transport, banking and financial services and health sectors.

3. Guiding Principles

The role of the State is to create a robust, stable and coherent regulatory framework for protecting networks and infrastructure enterprises and private persons and to support self-regulation in the private sphere. The principles that will be followed in this are set out below.

3.1 Rule of Law

We will focus on applying the rule of law, and will work to ensure that Irish citizens' rights under the Constitution and under the European Convention on Human Rights are preserved at all times.

3.2 Subsidiarity

Because of the diverse ownership and operation of various ICT systems, the State cannot assume sole responsibility for protecting cyberspace and the rights of citizens online. The owners and operators of information and communication technology are primarily responsible for protecting their systems and the information of their customers.

3.3 Risk Based Approach & Proportionality

Measures to increase the level of protection need to be informed by an assessment of the risks and threats facing us, as individuals, businesses, public sector bodies and the State as a collective whole. Furthermore such measures will need to be proportionate to the respective risks and threats that we face.

4. Objectives

- To improve the resilience and robustness of critical information infrastructure in crucial economic sectors, and particularly in the public sector.

- To continue to engage with international partners and international organisations to ensure that cyber space remains open, secure, unitary and free and able to facilitate economic and social development.

- To raise awareness of the responsibilities of businesses and of private individuals around securing their networks, devices and information and to support them in this by means of information, training and voluntary codes of practice.

- To ensure that the State has a comprehensive and flexible legal and regulatory framework to combat cyber crime by An Garda Síochána that is robust, proportionate and fair, and that accords due regard to the protection of sensitive or personal data.

- To ensure that the regulatory framework that applies to the holders of data, personal or otherwise, is robust, proportionate and fair.

- To build capacity across public administration and the private sector to engage fully in the emergency management of cyber incidents.

5. Measures

5.1 Establish the National Cyber Security Centre

We will formally establish the National Cyber Security Centre (NCSC) within the Department of Communications, Energy and Natural Resources. The NCSC will engage in a comprehensive set of tasks around cyber security, with primary focus on securing government networks, assisting industry and individuals in protecting their own systems, and securing critical national infrastructure.

The process of developing a Computer Security Incident Response Team (CSIRT-IE) commenced in the Department of Communications, Energy and Natural Resources in late 2011, on foot of a Government Decision. To date, CSIRT-IE has focussed on assisting public sector organisations in their response to computer security incidents and providing advice to reduce threat exposure. Some initial work has also been completed on the two other core future aspects of the work of NCSC.

Over the life of this Strategy, the skillset and constituency base of the NCSC will be developed as follows:

- The NCSC will seek formal accreditation for the Government CSIRT (g/CSIRT), which is critical in terms of peer recognition. This accreditation is expected in early 2016;

- Accreditation will be sought for a formal National CSIRT (n/CSIRT), while also developing a limited capacity in the area of Industrial Control and SCADA systems.

The mandate for the NCSC will include:

- activities to reduce the vulnerability of critical systems and networks within the State to incidents and cyber-attacks;
- effective response when such attacks occur;
- responsibility for the protection of critical information infrastructure (CIIP);

- establishing and maintaining cooperative relationships with national and international partners.

5.2 Network and Information Security for Public Bodies

We will introduce a series of measures to improve the network and information security used by Government Departments and Agencies, including a comprehensive incident reporting and escalation policy.

This will build on work already in progress involving an improved ability to detect and respond to threats and attacks. The evolution of attack vectors and threats has resulted in previous network security technologies becoming less effective and the adoption of a defence in depth approach. This involves the use of a wider range of devices and infrastructure in the service of network security. The NCSC's projects will ultimately yield such a system: a constituency wide, federated, Security Incident and Event Management (SIEM) system.

5.3 Fully implement the NISD by means of primary legislation

We will introduce primary legislation to give effect to the national cyber security arrangements and to transpose the proposed European Union Directive on network and information security. This process will be undertaken in a transparent and consultative manner, involving regulatory impact analysis and legislative scrutiny by the Oireachtas.

5.4 Coherent international engagement

We will continue to engage in European and global discussions on network and information security, including in the context of the global debate on the future of internet governance. We continue to emphasise the ongoing need for a secure, resilient internet architecture that fully encompasses the protection of fundamental rights online and which continues to facilitate economic and social development.

We will also engage at European and international levels with key partners in delivering policy measures to improve cyber security.

5.5 National Security and Policing

In recognition of its responsibilities for providing policing and security services to the State, it is envisaged that An Garda Síochána will be in a position to offer appropriate advice and guidance concerning preventative and investigative strategies. It will also be in a position to draw on its liaison relationships with other security services in identifying emerging threats, vulnerabilities and best practice preventative measures.

5.6 Cybercrime

The Minister for Justice and Equality will shortly bring forward legislation to give effect to the provisions of the Budapest Convention on Cybercrime and Directive 2013/40/EU on attacks against information systems. We will continue to work closely with that Department and the recognised legal and regulatory agencies including An Garda Síochána on the implementation of that legislation. This association will be formalised by means of a Memorandum of Understanding, setting out the respective roles and duties of each body.

5.7 Civil-Military Cooperation

The Defence Forces maintains a capability in the area of cyber security for the purpose of protecting its own networks and users. There is already a strong culture of cooperation between the NCSC and DF in areas such as development of technical skill sets, technical information sharing and exercise participation. These arrangements will be formalised by means of a Service Level Agreement with the Department of Defence, which will also include a mechanism for sharing technical expertise in the event of a national cyber incident or emergency.

5.8 Critical Infrastructure

We will continue to play a central role in the protection of critical national infrastructure, including through the national emergency management system overseen by the Government Taskforce on Emergency Planning and the Office of Emergency Planning in the Department of Defence. As such, the Department of Communications, Energy and

Natural Resources will operate as Lead Government Department for emergency situations relating to failures of, or attacks on, ICTs, and will operate in a secondary role to other Departments in cases where incidents may have a cyber-security dimension.

5.9 Information Sharing

The dynamic nature of the threat environment means that clear, open and rapid access and sharing of information across the full range of stakeholders is critical. CSIRT-IE has been developing strong bilateral relationships with similar organisations in other countries, and with ENISA, the European Network and Information Security Agency. Equally, the unit has a formal and active information sharing role with other public sector bodies, and with industry (including IRISS-CERT, a voluntary CERT).

The NCSC will expand its information sharing arrangements with national and international stakeholders, and will focus particularly on making information on developing issues public in a timely and relevant manner. In particular, the NCSC will engage with Internet Service Providers on a protocol that might be implemented to identify threats to the data and devices of their customers.

5.10 Education and training for Industry/SMEs

We will develop a programme of education and training, beginning with a revised Make IT Secure website to help citizens and Small to Medium Enterprises (SME) better protect themselves online. We will also develop a programme of structured exercises for critical national infrastructure owners and for public sector bodies, in partnership with international peers and the academic sector.

5.11 Public Awareness

We will work to foster a culture of cyber security across society, including through cooperation with the education system, with industry and through the promotion of events like European Cyber Security Month.

5.12 Relationships with Third Level Institutions

The Department of Communications, Energy and Natural Resources has a long standing relationship with the Centre for Cyber-crime Investigation in University College Dublin. We will continue to develop and deepen such partnerships with third level institutions through the use of Memoranda of Understanding to aid the sharing of knowledge, experience and best practice, and to support the developing research agenda in this sector.