ARTHUR COX

Group Briefing
May 2016

Ireland: Survey of Recent Developments in National Cyber Security Sphere

AUTHORS

PEARSE RYAN
PARTNER, TECHNOLOGY & INNOVATION
+353 1 618 0518
pearse.ryan@arthurcox.com

SHANE MCCARTHY
TRAINEE, TECHNOLOGY & INNOVATION
+353 1 618 0659
shane.mccarthy@arthurcox.com

INTRODUCTION

In this article, we consider recent policy and strategy level developments in the cyber security sphere in Ireland.

The World Economic Forum Global Risks Report for 2015[1] ranks technological risks, most notably cyber-attacks, among the most likely and impactful global risks. Cyber-crime and cyber-attacks, both nationally and internationally, have heightened awareness of these vulnerabilities and elevated cyber security to the national agenda. Along with other western economies, Ireland has taken the first organised national steps on the path to at least some degree of coherent national cyber security requirements.

Ireland has a developed infrastructure that is dependent on information and communication technologies (ICT). Critical national infrastructure such as energy, water, social welfare, telecommunications, banking and healthcare are dependent on ICT, not just to operate effectively, but to operate at all. Apart from indigenous companies nine of the top ten global software companies, all of the top ten global ICT companies and the top ten "*born on the Internet*" companies have major operations here. If a significant cyber-attack aimed at Irish operations should harm these companies, or any other large international company operating in Ireland, there is a recognised risk of damage to Ireland's reputation abroad as a suitable place to do business. Accordingly, the national ability to repel, or at least manage the response to, cyber-attacks is a recognised consideration in the ability of 'Ireland Inc.' to attract and retain inward investment.

National security can come under threat from international espionage or attempted sabotage of the software necessary to run critical infrastructure. The task of Government and industry is to ensure systems and networks are as safe as possible to inspire confidence and trust in the privacy of data and information so the digital economy can grow and prosper. Initiatives at EU and national level are response to the realisation that the EU has been losing ground due to the increased cyber security threat level, governments across Europe have been tasked with coming up with a national security strategy.

NATIONAL RISK ASSESSMENT

At national level, cyber security has been increasingly recognised as a risk which could threaten national progress, continued economic growth and prosperity. The National Risk Assessment for Ireland (2015)[2] published

1 http://reports.weforum.org/global-risks-2015/

2 http://www.taoiseach.gov.ie/eng/Publications/Publications_2015/National_Risk_Assessment_2015.pdf

by the Department of An Taoiseach (or department of the office of the Prime Minister) notes that cyber-attacks could potentially threaten Ireland's key national infrastructure (such as energy, transport and telecoms systems). The document also identifies the specific risk for the public service in respect of theft or compromising of data collected by the public service.

Although formal recognition of cyber security as a serious threat is welcomed, identifying risks is only a first step in properly addressing them and Government must ensure that these risks are dealt with through appropriate prevention and mitigation measures. The Government in recent months has taken a pro-active approach in developing a national strategy to combat cyber-threats.

NATIONAL CYBER SECURITY STRATEGY

On 3 July 2015, the Government, through the Department of Communications, Energy and National Resources, published the country's National Cybersecurity Strategy 2015–2017 (the "Strategy")[3]. The Strategy represents a high level policy statement from Government acknowledging the challenges with facilitating and enabling the digital economy and society. The Strategy is based on key principles such as the rule of law, subsidiarity, noting that we are ultimately responsible for our own security, and proportionality in response to key risks and threats facing us.

The Strategy, which sets out the Government's vision of a secure and reliable cyberspace to optimise and promote use of information systems for economic and social growth, outlines actions that will:

» continue to improve the resilience of networks in critical infrastructure and the public service;

» raise awareness of the importance of cyber security to business and citizens, and support them in securing their networks, devices and information;

» further develop a culture of cyber security across society, including through cooperation with the education system, industry and academia; and

» continue to build on Ireland's global reputation as a technology and information security hub, and help promote Ireland as the location of choice for ICT businesses.

Key measures outlined in the Strategy include:

» the introduction of a series of measures to improve the network and information security used by public bodies, including incident reporting and escalation policies;

» enacting legislation in order to allow Ireland to both ratify the Budapest Convention and transpose the EU Directive on Network and Information Security (the "NIS Directive")[4];

» co-operation with other nations including knowledge sharing and emphasising the need for secure and resilient infrastructure among policy makers;

» co-operating with key State Agencies, industry partners and international peers in the interests of protecting critical infrastructure, improving situational awareness and incident management along with facilitating education, training and public awareness initiatives;

» increasing the role of an Garda Síochána (the national police force) in respect of cybercrime preventative and investigative strategies;

» development of a national emergency management system in order to better protect Ireland's critical infrastructure (the authors regard this as a key measure);

» public awareness and education schemes to assist individuals and SMEs in better protecting themselves against cyber threats;

» education and training for SMEs;

» continue to develop and deepen 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; and

» co-operation between the National Cyber Security Centre and the defence forces in the area of cybercrime.

NATIONAL CYBER SECURITY CENTRE

To support the Strategy, the Government has established a National Cyber Security Centre (NCSC) within the Department of Communications, Energy and National Resources ("DCENR"), accredited to the Computer Security Incident Response Team (CSIRT-IE) which will be tasked with securing government networks, assisting both individuals and organisations with protecting their computer systems and protecting the country's critical infrastructure. Note that we are now discussing a third Department, which brings up an obvious concern in relation to inter-Department co-operation.

The NCSC will develop capabilities to respond swiftly when attacks occur and develop capabilities in the area of industrial control and SCADA systems, which are used to run utility sector control systems, such as apply to electricity and water networks. We discuss elsewhere the role of the NCSC pursuant to the NIS Directive.[5]

INTER-DEPARTMENTAL CO-OPERATION

The work of NCSC is supported by an Inter Departmental Committee on Cyber Security, established and chaired by the DCENR, which regularly reports on progress and on cyber security

3 http://www.dcenr.gov.ie/communications/SiteCollectionDocuments/Internet-Policy/NationalCyberSecurityStrategy20152017.pdf

4 for a discussion of the final text of the Directive see: (http://www.arthurcox.com/publications/agreed-text-of-the-directive-on-network-and-information-security/) and for a 2014 discussions of the then draft form of the Directive see: http://www.scl.org/site.aspx?i=ed39127

5 See footnote 4

issues to the Government Task Force on Emergency Planning. The Government Task Force, chaired by the Minister for Defence, maintains cyber security as a standing agenda item, allowing for provision of regular updates and addressing of issues of common interest.

Whilst the DCENR has lead responsibility relating to cyber security, the successful implementation of the Strategy requires effective inter-Departmental co-operation (which in Ireland as in any country appears to be a challenge). The Strategy places an emphasis on task-sharing and building trust relationships between the State, public and private partners, academia and civil society. It remains to be seen what protocols will apply to facilitate the flow of information.

For example, the Garda Síochána works closely with NCSC, both in a preventative and investigative capacity, with regards to national security and computer crime. It also liaises with international security services to help identifying emerging threats and vulnerabilities, and establishing best practice preventative measures. The Strategy outlines that this association will be formalised by means of a Memorandum of Understanding, setting out the respective roles and duties of each body.

There is a Memorandum of Understanding with the Centre for Cyber-crime Investigation (CCI) in University College Dublin. As a leading international centre for research and education in cybersecurity, cybercrime and digital forensics, the continued relationship with CCI is key to the success of the Strategy.

The Defence Forces also play a key role in the nation's defence against cyber-crime and are committed to participating, under the leadership of the DCENR, in the delivery of measures to improve the cyber security of the State, as proposed in the NCSC. The Communications and Information Services (CIS) Corps is responsible for cyber security within the Defence Forces. The CIS Corps, along with the Garda Síochána, provide significant domestic support role to the NCSC.

THE DEFENCE FORCES

Cyber security features prominently in both the Department of Defence Strategy Statement 2015–2017[6] and the White Paper on Defence which was published in August 2015[7], formally recognising that the broader concept of national security now encompasses the cyber security threat.

The Defence Forces not only leverage information sharing within the European military community which can be vital in our defence against cyber-attack, but also work with the Garda Síochána and DCENR in relation to the national response to cyber threat. It could well be argued that cyber threat is the most critical threat to national security.

The Department of Defence and the Defence Forces will provide support to the CSIRT-IE team in so far as resources allow. Two members of the Defence Forces are currently seconded to the CSIRT-IE. The issue of financial and personnel allocation is an underlying issue in the likely effectiveness of Ireland's organised national response to cyber threat.

It is expected that the Defence Forces role in assisting NCSC in the struggle against cyber-crime will be formalised through a service-level agreement, details of which are to be agreed between the Department of Defence and the DCENR. The agreement will likely include a rapid information sharing mechanism in the event of a national cyber incident or emergency.

NEXT STEPS

The Government are set to introduce primary legislation to give effect to the national cyber security arrangements. The Criminal Justice (Offences relating to Information Systems) Bill has been introduced and we have discussed it elsewhere[8]. This Bill will enable ratification of the Council of Europe Convention on Cybercrime and the transposition of the EU Directive 2013/40 on attacks against Information Systems.

The Strategy highlights that cyber threats exist for government and public utilities as well as for commercial entities and individuals. All businesses have a role to play in the successful implementation of the Strategy. All companies should ensure that they are "cyber-ready" and are urged to involve Government and An Garda Síochána both when planning for a breach and when dealing with the consequences of a breach.

The various initiatives discussed in this note reflect a mix of compliance with international and EU developments, together with home grown initiatives. The initiatives are at a legislative and policy level, rather than technical and project level. What we have not seen is a material allocation of public funding to strengthen or harden public sector ICT infrastructure, together with direct funding or indirect (via tax arrangements) funding of private sector ICT infrastructure. It remains to be seen whether, in the absence of material expenditure, policy and strategy, together with legislative, measures, will succeed in achieving absolute security of critical national infrastructure (almost impossible) or at least hardened infrastructure (possible but difficult to achieve). As we seen on an almost daily basis in the private sector, the preventative measures struggle to keep pace with the threat.

It is the view of the authors that government must be prepared to invest in schemes and initiatives to support public and private sector cyber security enhancement, whether via direct or indirect funding. This lack of funding can be compared with developments abroad, with obvious examples being the US and UK.[9]

6 http://www.defence.ie/website.nsf/Strategy2015E

7 http://www.defence.ie/WebSite.nsf/WP2015E

8 See discussion of bill at: http://www.scl.org/site.aspx?i=ed46808

9 For example, in November 2015 the UK government allocated £1.5 billion over five years "*to protect Britain from cyber attack and develop our sovereign capabilities in cyberspace. If you add together the spending on core cyber security capabilities, protecting our own networks and ensuring safe and secure online services, the governments total cyber spending will be more than £3.2 billion*".

FURTHER INFORMATION

For further information or specific advice regarding how the Regulation will impact your business, please contact any member of the Technology and Innovation team or your usual Arthur Cox contact:

JOHN MENTON
HEAD OF CORPORATE
+353 1 618 0558
john.menton@arthurcox.com

ROB CORBET
HEAD OF TECHNOLOGY & INNOVATION
+353 1 618 0566
rob.corbet@arthurcox.com

PEARSE RYAN
PARTNER, TECHNOLOGY & INNOVATION
+353 1 618 0518
pearse.ryan@arthurcox.com

COLIN ROONEY
PARTNER
+353 1 618 0543
colin.rooney@arthurcox.com

ISEULT MANGAN
ASSOCIATE
+353 1 618 1153
iseult.mangan@arthurcox.com

OLIVIA MULLOOLY
ASSOCIATE
+353 1 618 1160
olivia.mullooly@arthurcox.com

CHRIS BOLLARD
ASSOCIATE
+353 1 618 0649
chris.bollard@arthurcox.com

CLAIRE O'BRIEN
ASSOCIATE
+353 1 618 1124
claire.obrien@arthurcox.com

JOANNE NEARY
ASSOCIATE
+353 1 618 1114
joanne.neary@arthurcox.com

COLM MAGUIRE
ASSOCIATE
+353 1 779 4356
colm.maguire@arthurcox.com