The move to overhaul cyber security in Ireland

With the release on 2 July of its Cyber Security Strategy 2015-17, Ireland has taken an important step forward in advancing its cyber security agenda. The Strategy contains a number of provisions, including relating to legislation concerning cyber security; for example the Irish government through the Strategy makes clear that it will soon ratify the Budapest Convention. The objectives and initiatives found within the Strategy will be of note to businesses with operations in Ireland, which as Ireland's Government is keenly aware, includes many global technology and internet-born companies. Adam Finlay, Partner at McCann FitzGerald assesses the Strategy and what it means for Ireland's cyber security landscape.

Ireland's Cyber Security Strategy for 2015-2017 was published on 2 July 2015. It recognises the importance of cyber security to Irish citizens and businesses and sets out guiding principles, national objectives and measures to be implemented with a view to achieving those objectives. The measures include tangible actions such as the establishment of a National Cyber Security Centre ('NCSC') and the introduction of legislation dealing with cyber crime. However the Strategy acknowledges the limitations of what can be achieved through the unilateral efforts of the Irish Government. It therefore emphasises the need for engagement and cooperation on a domestic basis between the State, public and private partners, regulatory authorities, enforcement agencies, defence forces, academia and civil society and outlines how participation in international cyber security initiatives will be facilitated and managed in Ireland.

In its consideration of the importance of cyber security to Ireland, the Strategy focuses specifically on the digital economy and Ireland's international reputation, particularly in the ICT sector. It specifically mentions that 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 significant operations in Ireland and that, as a result, Ireland faces a more complex set of risks in connection with cyber security than many other countries. The same factors also give rise to unique opportunities. The Strategy states that there is a real potential for Ireland to become a cyber security hub on the basis of its developing cloud computing and big data sectors. It envisages the development of a cyber security industry being facilitated by the Irish Government and supported, in part, by R&D collaboration between industry and academic centres, such as the UCD Centre for Cybersecurity & Cybercrime Investigation. This approach may be contrasted with the UK's Cyber Security Strategy, which focuses more on GCHQ's cyber security expertise being an engine for the development of a commercial cyber security sector within the UK.

The principal objectives identified in the Strategy include: improving the resilience of critical information infrastructure; ensuring that Ireland has a comprehensive and flexible legal and regulatory framework to combat cybercrime that is robust, proportionate and fair; raising awareness of cyber security and engaging in cooperative initiatives to deal with cyber incidents. The Strategy envisages that the key measures to achieve these objectives will include the following:

- the establishment of the NCSC within the Department of Communications, Energy and Natural Resources. The NCSC is to focus primarily on: improving the security of government networks, assisting industry and individuals in protecting their own systems, and securing critical national infrastructure;
- the development of a security incidence and event management ('SIEM') system for public bodies;
- the introduction of primary legislation relating to cyber crime;
- continuing to engage in European and global discussions and initiatives on network and information security and sharing information with appropriate national authorities in other jurisdictions and EU bodies such as the European Network and Information Security Agency;
- fostering cooperation between public bodies and regulatory agencies, between the NCSC and the Irish defence forces and between the NCSC and third level institutions in connection with cyber crime, which will be formalised under memoranda of understanding and service-level agreements; and
- developing education, training and awareness programmes aimed at different stakeholders, including individuals, SMEs and critical national infrastructure owners.

The overhaul of Irish laws dealing with cyber security is particularly significant, since it is long overdue. Existing Irish legislation in this area is far from being 'comprehensive' or 'robust.' Instead it is a disjointed patchwork, consisting primarily of certain provisions of the Criminal Damage Act 1991, the Non Fatal Offences Against the Person Act 1997, the

Criminal Justice (Theft and Fraud Offences) Act 2001, the Criminal Justice Act 2011, the Data Protection Acts 1988 and 2003, the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, and the Postal and Telecommunications Services Act 1983 (as amended by the Interception of Postal Packets and Telecommunications Messages (Regulations) Act 1993). As the dates of these statutes would suggest, many of them were enacted at a time when current digital practices and cyber security issues could not have been envisaged, never mind appropriately addressed by the legislature.

The main piece of legislation referred to in the Strategy is the Criminal Justice (Offences relating to Information Systems) Bill which, according to the Government's legislative programme for 2015, is scheduled to be published later this year. Such a bill has, however, been on the legislative programme, in one form or another, since 2011. The principal purposes of this bill will be to enable the ratification of the Budapest Convention[1] and the transposition of the EU Cybercrime Directive[2]. The ratification of the Budapest Convention is long overdue, considering that it was signed by Ireland in 2002. The deadline for the transposition of the EU Cybercrime Directive is 4 September 2015 and it is perhaps this deadline that will provide the impetus required for this bill to be finalised and enacted. Once it is, the Garda Síochána (the Irish police force) and Irish regulatory and prosecution agencies ought to have a broader and more appropriately worded range of offences available to them to deal with cyber crime.

The overhaul of Irish laws dealing with cyber security is particularly significant, since it is long overdue

The Strategy also refers to the transposition of the proposed Network and Information Security ('NIS') Directive which, according to recent reports, has yet to be finalised but is expected to be adopted later this year. One of the stumbling blocks to the finalisation of the NIS Directive has been disagreement over the range of businesses that Member States will be obliged to bring within the scope of the NIS Directive's incident reporting regime. The extent to which digital service providers will fall within the scope of this regime is of particular relevance to Ireland due to the presence of many leading companies within this sector in Ireland. Although the deadline for the implementation of the NIS Directive is unlikely to be any earlier than 2017, it is clear that some of the measures set out in the Strategy are intended to address certain of Ireland's prospective obligations under the NIS Directive.

The Strategy recognises that cyber security is relevant to almost all sectors of the Irish economy but focuses, in particular, on the ICT sector and on critical economic infrastructure. Whilst it would have been impractical to name-check all industries in which cyber security is important, it is perhaps unfortunate that other data-centric sectors of strategic importance to the Irish economy, such as financial services, pharmaceuticals and medtech, were not mentioned. This is surprising considering that, for example, earlier this year the Central Bank of Ireland announced that its programme of themed inspections in market supervision would include assessments of regulated financial services providers' cyber security controls and procedures. In addition, although the Strategy is intended to benefit all Irish businesses, the SME sector is given scant attention. The main measures specifically targeted at SMEs are education and awareness campaigns, which will include a revised 'Make-IT-Secure' website. Given that SMEs are increasingly the targets of cyber crime, and considering the potential for cyber security weaknesses in SMEs to have major adverse impacts both for the relevant entities themselves and the broader business community and society, it is surprising that they received so little attention. However, it may be envisaged that the NCSC will focus more attention on the SME sector than the Strategy would suggest.

The publication of the Strategy is an important step in Ireland's evolving approach to cyber security. Given the importance of cyber security to the Irish economy, it is hoped that appropriate effort and funding will be allocated to the execution of the Strategy so that its commendable objectives can be achieved.

Adam Finlay Partner
McCann FitzGerald, Ireland
adam.finlay@mccannfitzgerald.ie

1. Council of Europe Convention on Cybercrime (23 November 2001).
2. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.