PLANNING AGAINST CYBER ATTACKS

With an increasing need for planners to be prepared for major disruptions in their areas resulting from cyber-attacks on state, council and private enterprise services, Michael Murphy, security intelligence consultant, writes that councils should test that they have the necessary resilience in their systems to maintain services.

While most attention has been focused on the introduction of the EU General Data Protection Regulations (GDPR), enforceable from 25 May 2018, there has been less attention paid to another piece of EU legislation, that being the Directive on Security of Network and Information Systems (NISD).

By 9 May 2018, the EU requires member states to adopt and publish laws, regulations and administrative provisions necessary to comply with the Directive, and are required to immediately inform the Commission that it has been adopted.

It is noted that the GDPR which is regulation must be incorporated into national law in its original form, the NISD on the other hand as a directive can be incorporated into national law in accordance with the spirit of the directive.

The NISD is the first EU-wide directive regarding cybersecurity and has a threefold objective: improve national level cyber security capabilities, increase co-operation across the EU, and, ensure risk management and incident reporting by operators. The directive once fully implemented should result in achieving a common level of security of networks and information systems throughout the EU.

To achieve the first objective states are required to: adopt a national strategy on the security of networks and information systems, designate National Competent Authorities (NCA) to monitor implementation of the NISD, designate a single point of contact to exercise a cross-border liaison function, and designate one or more Computer Security Incident Response Teams (CSIRTs).

REACTIVE CYBER SECURITY STRATEGY

Ireland already has a National Cyber Security Strategy (2015-2017) which is due for revision in 2018, and since 2011 it has established a National Cyber Security Centre and national CSIRTs within the Department of Communications, Climate Action and Environment. However, it should be noted that the current strategy is reactive rather than proactive and there is doubt as to the effective operation of the strategy.

Achieving the directive's second objective will be accomplished by the establishment of two groups. Firstly, the EU Co-operation Group composed of representatives of member states, the EU Agency for Network and Information Security (ENISA), and representatives from the EU Commission which will also act as the secretariat. The second group is the Network of national CSIRTs which will bring representatives of the national CSIRTs together.

These two networks will support and facilitate strategic cooperation and exchange information across the EU, which we are told will lead to trust, confidence, and effective operational co-operation between member states.

The directive's third objective will be achieved by the identification of two types of operational providers – Operators of

Essential Services. These are private or public entities that provide services that are considered to be essential for the maintenance of critical societal and/or economic activities.

They are divided into seven categories: energy service operators of electricity, oil, gas; transport services of air, rail, water, and roads; banking services; financial market infrastructures; healthcare; water; and digital infrastructure; secondly, Providers of Digital Services (DSP) which are categorised as persons or organisations that offer digital services at a distance, such as cloud computing services, online search engines, or online market places which if disrupted would cause widespread disruption.

INTERNATIONAL POLITICAL TENSIONS

This EU directive is coming at a time when international political tensions have risen and where cyber-attacks by states have become more sophisticated, more intense, and more aggressive.

These tensions are being played out in the virtual rather than the physical world, are invisible rather than visible, and where state or privately controlled networks face great risks. Future conflicts will be fought in civilian homelands where critical national infrastructure will be attacked as much as military forces.

No state is immune from this risk, even those not involved in the conflict. Cyber weapons do not wear a uniform or carry a national flag, cyber adversaries do not discriminate, and information systems discovered with vulnerabilities will be exploited.

The purpose of the exploitations can be grouped under four 'S' categories: Spying, Sabotage, Subversion and Stealing. Spying or espionage is most common where weaknesses are identified. Information is stolen and reconnaissance is performed for future attacks. Sabotage is conducted to attack and/or cripple a nation's critical national infrastructure, these were previously listed above.

The effects of these attacks can completely disrupt normal living and the attack can continue for indefinite periods. The most famous of these attacks were conducted against Estonia in 2007. Subversion attacks may be part of an information operations or influencing campaign attempting to influence public opinion, undermine democracy or attack a political system.

Stealing of information, for example, can result in a state, corporation, or individual gaining an economic advantage and being the first to market with the production of innovative products, or stealing personal information that can be exploited for later economic or security gain. In the USA, for example, it is believed that 21 million records of US citizens and five million fingerprints were stolen from the Office of Personnel Management by another state.

REAL AND PRESENT DANGER

Cyber threats are real and are present. In the cyber world Ireland is no longer an island. Its channels of communications go through neighbours' territories and its borders are in the virtual world. The cyber threat is the greatest threat to our national security.

The risks flowing from those threats are enormous and can cripple this country adversely impacting on citizens, foreign direct investment, financial well-being, and national reputation.

Pat Larkin, CEO of Ward Solutions, recently wrote, and it would be hard to disagree, that *'Ireland's strategy is reactive and compliance-based, focused on meeting guidelines laid out in the European directive…Ireland currently ranks high on indices measuring our vulnerability to cyber-attack and low on benchmarking levels of cyber security maturity'.*

To adapt a well-known quote, the cyber threat does not stop at the Red Cow Roundabout. It is something that not alone must be considered by the national government but also the city and county councils.

ABOUT THE AUTHOR

Michael C. Murphy spent over 40 years in the Defence Forces before retiring in 2013 as Deputy Director of Military Intelligence at the rank of Lieutenant Colonel. During his early officer career he served in operational and intelligence roles on the border facing South Armagh.

Subsequently he held intelligence, operational and command roles, at Defence Forces Headquarters and the 2 Eastern Brigade before returning to Defence Forces intelligence where he completed his career.

During his career he served in overseas operational and command appointments with the UN and NATO in Lebanon (1978, 1986, 1991) Eritrea (2002) Afghanistan (2006) and Kosovo (2008). His extensive operational and intelligence experience is complemented by several educational and training qualifications earned at home and abroad, including a Diploma in Strategic Intelligence, and an MSc in Security and Risk Management at the University of Leicester.

Since retiring from the military he has provided security intelligence consultancy services to private industry and has become a leading commentator across the Irish media on security and intelligence issues.

He is founder and CEO of SITARMS Ltd, which provides accurate, timely, and comprehensive security intelligence, threat and risk management services. For details visit www.sitarms.com