Improving Cybersecurity in the European Union: The Network and Information Security Directive

By Richard Tauwhare

Welcoming the agreement in December 2015 on the draft text[1] of the first EU-wide legislation on cybersecurity, the European Commission Vice-President for the Digital Single Market, Andrus Ansip, said: "If we want people and businesses to use and make the most of connected digital services, they need to trust them to be secure in the case of attack or failure. The Internet knows no border—a problem in one country can have a knock-on effect in the rest of Europe. This is why we need EU-wide cybersecurity solutions."[2]

The proposed directive would impose closer cooperation between Member States, a minimum level of security for networks and services across the European Union, and mandatory reporting of significant cyber incidents by certain organizations, including operators of critical infrastructure (digital, energy, transport, financial services, healthcare) and providers of digital services (search engines, cloud providers, and major ecommerce Web sites).

Data protection laws already require companies to have adequate security measures when processing personal data, so these measures can be seen as an extension of current laws.

But network and information security is an increasingly important precondition for economic growth and national security. More and more it is subject to threats including human error, natural events, technical failures, and malicious attacks. Cybercrime in particular is growing in magnitude, frequency, and sophistication, while the distinction between attacks by governments, terrorists, and criminals is blurring. It is estimated that in 2015:

- The annual cost to the global economy from cybercrime and cyberespionage was over $445 billion;
- The 15 largest documented attacks worldwide involved the theft of the personal data of more than 300 million customers; and
- Over 90 percent of large organizations in the United Kingdom suffered some form of cyberattack.

Security incidents threaten not only financial harm, disruption, reputational damage, litigation, and loss of intellectual property but also safety, essential services, and national security. Disruption in one country can affect many others. For the European Union, the resilience and stability of network and information systems is seen as essential to the completion of the Digital Single Market and the smooth functioning of the Internal Market.

This article examines the key EU proposal to address these challenges: the Network and Information Security Directive (NISD). It considers in particular which companies will be affected and what they will need to do to comply with the new regulatory framework that the NISD will establish.

CONTEXT

Many EU governments have voluntary schemes and national advisory bodies to help companies identify and mitigate cyber risks. For the great majority of companies, the reporting of incidents is voluntary rather than compulsory. In the United Kingdom, the Information Commissioner's Office has issued

Richard Tauwhare *is a Senior Director in the International Trade practice at Dechert LLP in London, England. He specialises in advice on UK and EU trade-related regulations. Mr. Tauwhare is a former senior UK diplomat with 35 years' experience of negotiating and implementing international trade-related agreements.*

guidance that if a breach of personal data meets certain conditions then it should be notified by the company; the Financial Conduct Authority also expects regulated firms to notify it of breaches. The UK's "Cyber Essentials"[3] program and the National Cyber Security Centre[4] provide guidance and a voluntary framework as part of a $2.6 billion program by the UK Government between 2015–2020 to defend against cyberattacks.

But the authorities' patience with voluntary measures is running thin in the face of the growing scale of the threat and the continuing failure of companies to take adequate steps to protect themselves and the data they hold.

Within the European Union, current regulation is based on a fragmented patchwork of national legislation. A recent report[5] finds that while some Member States have relatively strong cybersecurity legal frameworks—the United Kingdom, Germany, and Estonia, for example—others still have much to do. The discrepancies between Member States' laws and operational capabilities pose a threat to the entire Single Market and the overall network security of the European Union is weakened by those Member States with an insufficient level of protection.

Among the gaps is a lack of cooperation both between governments themselves and between governments and the private sector. Current government-to-government cooperation is limited to a minority of Member States with a high level of capabilities. The differences in approach between the Member States create space for uncoordinated regulatory interventions, incoherent strategies and divergent standards, with cybersecurity potentially used as justification for protectionist rules that reduce choice and undermine cyber protections. This also may result in insufficient protection for networks across the European Union and compliance costs for companies operating in more than one Member State.

Current EU regulations require only telecommunication companies to adopt risk management steps and to report serious network and information security incidents. But many other sectors also manage critical infrastructure or provide essential services. However, only five EU Member States have an established framework for public-private partnerships on cybersecurity and, across the European Union, these sectors lack clear and robust obligations to adopt risk management measures and exchange information with the authorities. As a result, businesses lack incentives to take the steps necessary to ensure the security of their networks and many incidents go unreported, leaving the authorities with inadequate information on which to base mitigating measures and strategic priorities.

To address these concerns, in 2013 the European Commission set out an EU Cybersecurity Strategy[6] alongside its Digital Single Market Initiative.[7] The Strategy aims to:

- promote cyber resilience;
- reduce cybercrime;
- develop cyber-defense policies and capabilities; and
- establish a coherent cyber policy for the European Union.

The NSID is the main action of the Strategy. The other key related action is the General Data Protection Regulation[8] that will strengthen EU citizens' privacy protections and streamline regulation across the 28 Member States, again replacing the existing patchwork of national rules. Further actions under the Strategy will include raising awareness, developing an internal market for cybersecurity products and services, fostering Research & Development investment and stepping up the fight against cybercrime.

TIMINGS

The text of the Directive provisionally was agreed on December 18, 2015. The European Parliament's Internal Market and Consumer Protection committee voted in favor of the Directive on January 14, 2016. It was approved by the Council of Ministers in May and the European Parliament is expected to give its formal agreement by August. The text will then be published in the Official Journal of the European Union and will enter into force 20 days from the date of its publication. The deadline for transposition in the laws of the Member States will be 21 months coming into force of the Directive. Member States will then have a further six months to identify operators of essential services established in their territory.

OBJECTIVES OF THE NISD

The NISD will be the first-ever EU cybersecurity legislation. In its Explanatory Memorandum[9] on the Directive, the European Commission states that:

> The aim of the proposed Directive is to ensure a high common level of network and information security … This will be achieved by requiring the Member States to increase their preparedness and improve their cooperation with each other, and by requiring operators of critical infrastructures … to adopt appropriate steps to manage security risks and report serious incidents to the national competent authorities.

Its provisions are similar to those in the US Cyber Security Framework but it will establish mandatory rather than voluntary requirements. There are no current EU plans to mirror the US capacity to impose sanctions on foreign individuals and groups that use cyberattacks to threaten security or economic interests (although to date the US capability has yet to be exercised).

The Directive will impose three different sets of obligations on: (1) governments, (2) operators of essential services, and (3) digital service providers. The following examines each of these as well as general requirements that will apply more broadly and the consequences of the Directive for both EU and non-EU companies.

EU MEMBER STATE GOVERNMENTS

The NISD will impose four main obligations on all Member States.

1. All EU governments will be required to adopt a Network and Information Security Strategy, if not in place already. This will define each government's strategic objectives and the appropriate policy and regulatory measures it will take to achieve and maintain a high level of security.
2. Governments must designate a national point of contact and competent authority or authorities, to monitor the application of the Directive in their territory and to contribute to its consistent application throughout the European Union. Member States may designate this role to an existing authority or authorities. It will have the power to require the operators of essential services and digital service providers to provide the information needed to assess the security of their networks and information systems.
3. Member States must set up Computer Security Incident Response Teams (CSIRTs), which will be responsible for handling risks and incidents.
4. Member States are required to co-operate, both with each other and with the European Union Agency for Network and Information Security (ENISA). There will be a network of the national CSIRTs, composed of representatives of Member States' CSIRTs and CERT–EU (the Computer Emergency Response Team for EU institutions, bodies and agencies), with the Commission participating as an observer, to promote swift and effective operational co-operation by, amongst other things, exchange of information and supporting Member States to address cross-border incidents on a voluntary basis.

Following debate, the European Parliament broadly has accepted the Council's preference for voluntary cooperation and information sharing. There will be a limited requirement to share information on incidents that would impact on the continuity of service in another Member State. But earlier more radical proposals requiring Member States to give early warning of significant threats have been replaced with tasking the CSIRTs with discussing further forms of operational cooperation, including on early warnings and coordinated responses.

There remain some concerns that the Directive provides inadequate practical guidance on how national competent authorities should ensure consistent application of the Directive in each Member State nor how this should be coordinated across Member States. This risks allowing long-standing differences of approach to persist, for example, between Germany and France, on the one hand, which traditionally have supported legislating for cybersecurity and the United Kingdom, on the other hand, which has preferred a non-interventionist and industry-led approach.

OPERATORS OF ESSENTIAL SERVICES

There was considerable debate between the Commission, Parliament, and Council over the degree of discretion to be allowed to Member

States in selecting the key operators within selected industries to whom the new rules would apply. But, notwithstanding continuing concerns that this could result in a fragmented rather than harmonized implementation of the Directive by Member States, the outcome is that each Member State will have national discretion to draw-up a list of these organizations. (The lists need not be published, for national security reasons). The key criteria for selection will be as follows:

- That an organization will be conducting effective and real exercise of activity through stable arrangements on the territory of a Member State (branches and subsidiaries will be included within this definition);
- That an organization will be providing a service that is essential for the maintenance of critical societal and/or economic activities;
- That the service depends on network and information systems; and
- That an incident affecting the network and information systems of that service would have significant disruptive effects on its provision.

When determining the significance of a potential disruptive effect, a Member State will take into account sectoral and cross-sectoral factors:

- Number of users relying on the service;
- Dependency of other essential sectors on the service;
- Impact that incidents could have on economic and societal activities or public safety;
- Market share of the entity;
- Geographic area that could be affected by an incident; and
- Availability of alternatives for the provision of the service.

Designated Sectors

Annex II of the NISD lists or cross-references the types of entities in the following designated sectors that may qualify as operators of essential services:

- **Digital infrastructure**—Internet exchange points, top-level domain name registries, and domain name system service providers (but not e-commerce platforms). An Internet exchange point is defined as "a network facility that enables the interconnection of more than two independent autonomous systems, primarily for the purpose of facilitating the exchange of internet traffic."
- **Energy**—Electricity suppliers and operators of systems for electricity distribution, transmission and storage; liquefied natural gas system operators, companies responsible for the production, transmission, distribution, supply, purchase or storage of natural gas, and operators of natural gas refining and treatment facilities; operators of oil transmission pipelines, oil production, refining and treatment facilities, storage and transmission.
- **Transport**—Airlines, airports manages and organizations that operate ancillary installations within airports, including air traffic control service providers; managers of rail infrastructure and licensed rail transport operators; road traffic management control and intelligent road transport system operators; ferry operators and other inland, sea and coastal passenger and freight water transport companies; bodies that manage ports, port facilities and works and equipment contained within ports; and operators of vessel traffic services;
- **Financial services**—Banks and other credit institutions (defined under existing EU legislation as "an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account"), operators of trading venues, including regulated markets such as, the London Stock Exchange and other multilateral (*e.g.*, the Alternative Investment Market in London) or organized trading facilities.
- **Healthcare and drinking water**—Hospitals, General Practitioner surgeries, private clinics, as well as, potentially, private sector healthcare businesses; suppliers and distributors of water intended for human consumption (although distributors for whom distribution of water for human consumption is only part of their general activity will be exempt).

Telecommunications companies already are regulated under the Framework Directive for electronic

communications (2002/21/EC) and are therefore excluded from the NISD.

Obligations

Organizations identified as operators of essential services must fulfill two main requirements (regardless of whether they perform the maintenance of their networks and information systems themselves or outsource the work).

First, they must put in place appropriate and proportionate risk management measures to prevent and minimize the impact of incidents that affect the security of their networks and information systems, with a view to ensuring the continuity of those services.

Second, operators of essential services must comply with a reporting scheme, to be established by each Member State, under which they must notify without undue delay incidents having a significant impact on the continuity of the essential services they provide. "Incidents" are defined as those events that have an actual adverse effect on the security of networks and information systems.

The Directive establishes criteria to be taken into account when assessing the impact of any incident, including the number of users affected, the duration of an incident and its geographical spread. Member States have been granted some discretion to develop national, sector-specific guidelines on what constitutes a reportable incident, enabling differences between states and sectors to be taken into account. But EU-level discussion will aim to avoid the development of widely-divergent approaches. Competent authorities acting together within the cooperation group may adopt guidelines on the circumstances in which operators of essential services are required to notify incidents, including on the parameters to determine the significance of the impact of an incident.

DIGITAL SERVICE PROVIDERS

Unlike the provisions for designating operators of essential services, the Directive does not allow discretion to Member States governments to determine which digital service providers fall within the regulations. Instead, the Directive will "apply to all digital service providers within its scope." These will be those organizations that:

- Have their main establishment in a Member State—defined as when they have their head office in the European Union in that Member State. Establishment implies the "effective and real exercise of activity through stable arrangements;"
- Are not established in the European Union but that offer services within the European Union. These organizations must designate a representative in one of the Member States where the services are offered. "Offering services" will be indicated by factors such as the use of a language or a currency generally used in one or more member states with the possibility of ordering services in that language, and/or the mentioning of customers or users in the European Union;
- Have fewer than 50 employees and whose annual turnover and/or annual balance sheet does not exceed EUR10 million, will not have certain requirements apply. (There is no equivalent size threshold in respect of operators of essential services.)

Services

There were substantial differences between the Commission, Parliament, and Council over which digital services should be included within the scope of the Directive. The result, set out in Annex III of the Directive and the corresponding recitals, reflects a compromise that excludes a number of significant services. Those scope are as follows:

- **Online marketplaces—**Services that allows consumers and/or traders to conclude online sales and service contracts with traders either on the online marketplace's Web site or on a trader's Web site that uses computing services provided by the online marketplace. This includes App stores but not price comparison Web sites, that is, online services that compare products or services and redirect the user to the preferred trader.
- **Online search engines—**Services that allow the user to perform searches of all Web sites, or all Web sites in a particular language, on the basis of a query, but not search functions that are limited to the content of a specific Web site.
- **Cloud computing services—**Services that enable access to a scalable and elastic pool of shareable computer resources. This means computing

services that can respond to an increase or decrease in demand for resources or processing power from multiple users accessing the service in different geographical locations, but where the processing is carried out separately for each user, although the service is provided from the same electronic equipment.

Obligations

The Directive provides for lighter touch harmonized rules across the European Union for digital service providers than for operators of essential services, allowing them greater flexibility to select their own, proportionate risk management approaches and avoiding the imposition of multiple different reporting regimes. These organizations will be required (regardless of whether they perform the maintenance of their networks and information systems themselves or outsource the work) to:

- Take appropriate and proportionate measures to manage risks taking into consideration: the security of systems and facilities; incident management; business continuity management; monitoring, auditing and testing; and compliance with international standards;
- Take measures to ensure the continuity of their services by preventing and minimizing the impact of incidents;
- Notify any incident that has a substantial impact on the provision of a digital service. The Directive establishes parameters to be taken into account when assessing the impact of any incident including the number of users affected, the duration, the geographical spread, the extent of the disruption, and the impact on economic and societal activities. The obligation to notify an incident shall only apply when the digital service provider has access to the information required to appreciate if the criteria are fulfilled.

When an operator of essential services relies on a digital service provider for the provision of a service that is essential for the maintenance of critical societal and economic activities, any significant impact on the continuity of the essential services due to an incident affecting the digital service provider shall notify the operator of essential services.

GENERAL REQUIREMENTS

NOTIFICATIONS

Because the degree of risk generally is lower for digital service providers than for operators of essential services, they face less stringent obligations. In particular, they only need to report security incidents that have "a *substantial* impact on the provision of a service …". In contrast, operators of essential services must report "incidents having a *significant* impact on the continuity of the essential services they provide."

If an operator of essential services or a digital service provider gives notice of an incident:

- The notice should include information to enable the competent authority to determine any cross-border impact of the incident and to inform other affected Member States if the incident has a significant impact;
- After consulting the entity making a notification, the competent authority may inform the public if it judges this necessary either to prevent an incident or to deal with an on-going incident. With respect to notifications by digital service providers only, the competent authority has an additional discretion, after consultation with the notifying party, to inform the public where such a disclosure is judged to be in the public interest; and
- The entity making a notification will not be obliged to notify any other parties such as customers, employees, or law enforcement agencies. However, they should consider whether there are any parallel requirements also to report the same incidents, for example, under the new General Data Protection Regulation if the incident concerns a breach of personal data and/or to financial services regulating bodies for incidents compromising the integrity of client data or impacting the continuity of services. This creates a number of potential issues including managing different triggers for reporting of breaches, with different timing expectations. The recitals recognize this potential for administrative burden and suggest that ENISA could co-operate with personal data protection authorities and assist in the production of guidelines to facilitate the reporting of incidents compromising personal data.

In the event that a competent national authority decides to inform other Member States and/or the public about an incident, the notifying party's security and commercial interests, and the confidentiality of any information it has provided, will be preserved. Notification will not expose the notifying party to increased liability.

Entities that are outside the scope of the Directive may notify incidents with a significant impact on the continuity of their services on a voluntary basis. This will not have the effect of imposing on them the obligations under the Directive (but it might in due course lead to a broadening by convention, or pursuant to regulatory or industry guidance, of the reporting requirements of the Directive). Member States will be required to process voluntary notifications only if it does not constitute a disproportionate or undue burden on the Member State concerned, and they should prioritize the processing of mandatory notifications over that of voluntary notifications.

ENFORCEMENT AND PENALTIES

Competent national authorities may require operators of essential services and digital service providers to provide the information needed to assess the security of their networks and information systems.

Operators of essential services (but not digital service providers) also must provide evidence to competent national authorities of the effective implementation of their security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, make the results, including the underlying evidence, available to the competent authority. Following the assessment of either the information provided by an operator of essential services or the results of a security audit, the competent authority may issue binding instructions to the organization concerned to remedy their operations.

Digital service providers are to be subject only to reactive ex-post supervisory activities by the competent authorities, which will take action only when they have evidence that a digital service provider is not complying with the requirements of the Directive. Such evidence may be provided by the digital service provider itself, by a competent authority, including a competent authority of another Member State, or by a user of the service. The competent authority may require that digital service providers remedy any failure to fulfill the requirements to take appropriate and proportionate measures to manage the risks to the security of their networks and information systems.

The Directive requires Member States to make and enforce "effective, proportionate and dissuasive" penalties. These penalties, and the agencies responsible for enforcing them, will be defined by each Member State.

STANDARDIZATION

The Directive requires Member States to encourage the use of EU or other internationally-accepted standards for the security of networks and information systems. ENISA may work with Member States to produce advice and guidelines on the technical areas which should be considered. The recitals suggest that it may in due course be necessary to draft harmonized standards to ensure a high level of security at an EU level.

Individual Member States may not establish a lower level of requirements than those set out in the Directive. However, with reference to operators of essential services only, Member States may set higher standards within their national legislation, which may lead to differences between the Member States.

CONSEQUENCES FOR COMPANIES

Although the provisions of the Directive will not enter into force for companies until at least 2018, and the exact standards to be adopted by each Member State have yet to be defined, businesses should be proactive in preparing for their implementation.

Because the Directive will impose in most cases the first mandatory requirements for notification of cybersecurity breaches, the risk of significant damage to a company's reputation and brand will be added to the other severe risks imposed by such breaches, particularly if a breach is poorly-handled.

As a first step, organizations active in the fields listed above should consider whether they are liable to come within the scope of the Directive either as operators of essential services or as digital service providers.

If this is or is likely to be the case, such organizations should identify under which Member States' jurisdiction they will fall. Those operating in more than one EU country should clarify in which Member State they have their "main establishment." Organizations not established in the European Union but offering services within it should consider in which Member State they wish to designate a representative to act on their behalf.

Such organizations should, to the extent that this is not done already on a regular and comprehensive basis, assess the risks they face and conduct a full review of the protections in place against deliberate attack, accidental loss, or other potential means by which their services could be breached or disrupted. This analysis should include consideration of key areas including access controls and policies, and system and network separation, to keep sensitive information separate.

The results of the review should be followed-up by the adoption and implementation of a new or revised, proportionate company-wide cybersecurity policy. This should include:

- Proactive measures continuously to scan for vulnerabilities and to address them;
- Preparing and regularly testing (internally or with the help of an external auditor or counsel) an incident response plan to detect and contain threats rapidly, and to minimize their impact. This should include co-ordination, communications, forensic investigation, reporting and recovery, as well as procedures to assess the significance of incidents against the criteria in the Directive to determine whether a notification may be required. The members and back-up members of an independent response team should be identified and should understand their respective roles, responsibilities, and decision-making authorities;
- Ensuring that suppliers and their subcontractors implement security measures and provide regular, robust evidence that these are appropriate, effective, and take account of the latest technological developments; and
- Training and awareness programs to ensure that relevant employees and suppliers understand what they need to do to keep the company and its data secure, are aware of the policy and the response plan, and are equipped to implement them.

Under existing duties of care and as a matter of corporate responsibility, or (in the case of listed companies) stock exchange rules, some businesses already may be required to assess these risks and take appropriate measures. Nonetheless, it would be prudent for such businesses to refresh their cybersecurity policies, procedures, and checklists, possibly after consulting with the competent authority or CSIRT.

This also may be required by a company's insurers if it holds cyber-risks insurance, although it generally is not advisable to accept an insurance policy if coverage is excluded in the event of noncompliance with an internal policy or procedure.

CONCLUSION

As with much EU legislation, the originally more comprehensive vision of the European Commission has been narrowed and amended to reflect compromises with the European Parliament and Council. While EU Directives always are subject to some national differences in application, the NISD particularly is prone to inconsistencies as it leaves much of the detail to be determined by individual Member States in their implementing legislation. This risks lessening its impact.

Nonetheless, the introduction of these measures will mark a significant step in promoting greater resilience and a more coherent response to cyber threats in Europe, in requiring key organizations to meet minimum harmonized standards of security and in obliging them to report serious incidents.

Günther Oettinger, European Commissioner for the Digital Economy and Society, said: "Cybersecurity is essential in today's European digital economy and society—and it remains a permanent challenge. We will remain active in this area…" The adoption and implementation of the NISD, in parallel with the General Data Protection Regulation, will represent first important steps. But given the rapidly-evolving and growing nature of the threat, the European Union is likely to need to coordinate more closely, to anticipate new risks more perceptively, and to take action more proactively if it is to maintain the secure cyber environment that is increasingly a cornerstone

of the EU's Single Market and a key driver of its economic growth.

NOTES

1. The draft text agreed on December 18, 2015 is available here: *http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-cybersecurity-agreement/?utm_source=dsms-auto&utm_medium=email&utm_campaign=EU+steps+up+cybersecurity%3a+member+states+approve+agreement*.
2. European Commission press release December 8, 2015 *http://europa.eu/rapid/press-release_IP-15-6270_en.htm*.
3. Cyber Essentials is a voluntary scheme through which companies can receive certification that they have taken basic precautions. Certification is now mandatory for companies bidding for higher-risk government contracts and this requirement is likely soon to be extended to all government contractors. *See https://www.gov.uk/government/publications/cyber-essentials-scheme-overview*.
4. The National Cyber Security Centre, due to open in London in October 2016, will bring together cyber expertise "to transform how the UK tackles cyber security issues." One of its first tasks will be to work with the Bank of England to produce advice for the financial sector. It will also include a Cyber Security Operations Centre to protect Ministry of Defense networks and systems. *See https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together*.
5. *http://cybersecurity.bsa.org/index.html*.
6. The EU Cyber Security Strategy 2013: *https://ec.europa.eu/digital-single-market/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security*.
7. The EU Digital Single Market Initiative: *https://ec.europa.eu/digital-single-market/en/digital-single-market*.
8. Reform of the EU data protection rules and the General Data Protection Regulation: *http://ec.europa.eu/justice/data-protection/reform/index_en.htm*.
9. *http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013PC0048*.