Possible sanctions

Chapter V of the Directive requires Member States to adopt 'effective, proportionate and dissuasive' sanctions for non-compliance. The Directive does not prescribe the form of such sanctions, though it seems likely that they will be of a similar to existing regulatory punishments (e.g. a fine, a 'name-and-shame' type notice, etc).

Conclusion

Cyber threats are becoming increasingly prevalent in society today. The interconnected nature of our networks means that individual States cannot assess their cybersecurity in isolation from the rest of the digital marketplace. The overarching purpose of the Directive - to establish a common minimum standard of network security across Europe - should therefore be viewed as a legitimate aim.

One might still question the worth of the Directive in the context of the global digital market. The Commission's foreword to the Directive recognises that Europe's overall network resilience can be weakened by an individual Member State deploying insufficient levels of cybersecurity. Could the same not be said for the rest of the world? What benefit is a uniform security standard in Europe when the likes of Asia and the Americas do not follow suit?

If implemented successfully, the Directive could represent an opportunity for Europe to set a benchmark on cybersecurity for the rest of the world to follow. However, in its current form, the Directive contains a number of flaws, the foremost being that key concepts are left open to interpretation by Member States (such as the meaning of 'public administrations' and 'significant impact'). These grey areas could lead to the Directive being adopted inconsistently, causing a real headache for businesses that operate in multiple jurisdictions. It remains to be seen whether these issues will be resolved before the Directive is adopted.

It will also be of interest to the business community to see how the Directive is implemented at a national level. Member States should be careful not to place unnecessary burdens on the businesses when introducing their own cyber regulations.

Importantly, businesses should be alert to the requirements that they could potentially face in the future, particularly with regards to notification and information sharing. Commercial contracts today typically include terms on data protection and other regulatory requirements, and with the Directive in mind, express contractual provisions on cybersecurity may become more common. Before entering into any long-term contractual arrangements, business leaders should ask themselves: could my organisation be caught by the scope of the Directive? If the answer is yes, appropriate steps should be taken to 'futureproof' their contracts.

Contacts

Simon Shooter
Partner
simon.shooter@twobirds.com

Joseph Jackson
Associate
joseph.jackson@twobirds.com

Toby Bond
Associate
toby.bond@twobirds.com

twobirds.com

Abu Dhabi & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Düsseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Skanderborg & Stockholm & Warsaw

0001257-01

Bird & Bird & Cybersecurity and the EU: regulating for network security

On 7 February 2013 the European Commission published its cybersecurity strategy by which it aims to ensure a common level of network information security across the European Union. The strategy sets out the Commission's aims on improving Europe's network resilience, which include raising awareness of the issues surrounding cybersecurity, developing an internal market for cybersecurity products and services and fostering R&D investment. Published alongside the strategy, and forming its main action, is a draft Directive ("the Directive") setting out a number of proposals designed to enhance the European Union's resilience to cybersecurity threats.

Whilst still at an early stage, and with national implementation of any binding rules still some way off, the Directive gives an indication of how regulation in this area may develop over the coming years. In particular it suggests a greater focus on cybersecurity as part of organisational risk management. It is important that businesses are aware of the Directive and its likely implications so that they are well placed to manage regulatory change in the future.

Current regulation

The current regulatory landscape on cybersecurity has evolved piecemeal over time and is drawn from a number of sources including:

- Data protection rules requiring businesses in the EU to implement appropriate technological and organisational security measures against unauthorised or unlawful processing, accidental loss, and destruction or damage of personal data;
- The Electronic Communications Framework Directive and the Privacy and Electronic Communications Directive requiring public electronic communication service and network providers to ensure the security of their services and networks and report serious network security breaches to their national regulators; and
- The Markets in Financial Instruments Directive requiring those in the financial services industry to adopt adequate risk management systems which by implication includes the adoption of network security risk management measures.

The Directive - an overview

At its core the Directive has two aims. The first is to ensure that Member States and those private undertakings providing certain critical infrastructure within the EU have an adequate strategy, and take appropriate steps, to deal with cybersecurity threats. The second is to facilitate information sharing about cybersecurity threats between the public and private sectors and between Member States. The Directive also sets out in broad terms the obligations that Member States will be expected to impose at industry level.

National strategy

Chapter II of the Directive sets out proposed requirements on the establishment of national frameworks for network information security planning. If adopted, the proposals would require each Member State to:

- adopt a national strategy and cooperation plan regarding network and information security;
- establish a national competent authority ("NCA") tasked with monitoring the application of the Directive. NCAs will also be required to 'contribute to [the Directive's] consistent application' across Member States, though it is unclear what this will require NCAs to do in practice; and
- establish a Computer Emergency Response Team ("CERT") to work under the supervision of its NCA. The role of CERTs appears to be more 'hands-on' than that of the NCAs and includes monitoring and responding to cybersecurity incidents, raising public awareness of cyber risks and forging cooperative relationships with the private sector.

Cooperation and Information Sharing

Chapter III of the Directive sets out plans for establishing a communication network, aimed at providing 'permanent communication' between NCAs and the Commission. It is intended that the communication network will be used to:

- circulate early warnings of cyber risks and incidents. The Directive would oblige NCAs to report risks and incidents that affect multiple Member States, as well as those that 'exceed national response capacity' or could 'grow rapidly in scale'. There is a risk that in practice, Member States might apply differing thresholds as to what sort of incident would trigger notification;
- facilitate a coordinated response to cyber threats. The Directive simply states that NCAs must 'agree' on a response, though it does not make clear what would happen in the event that agreement cannot be reached. Furthermore, the effectiveness of any response could be undermined if delays are caused by having to get each Member State's approval; and
- exchange information and best practices. The Directive envisages non-confidential information being made available through a common website and sensitive information being exchanged via a secure infrastructure.

Impact at industry level

Chapter IV of the Directive sets out the minimum obligations that Member States will be expected to impose at an industry level. It is this section of the Directive which is likely to generate the most debate.

Who will be affected?

The Directive requires that Member States impose the Chapter IV obligations on certain 'market operators' who provide:

- 'critical infrastructure', such as the energy, health, transport and financial services sectors; and
- 'information society services which enable the provision of other information society services', which includes e-commerce platforms, online payment gateways, social networks, search engines, cloud services and app stores.

The Directive envisages that the Chapter IV obligations shall not be placed on so called 'microenterprises', or in other words, businesses with fewer than ten employees and with an annual turnover of €2 million or less.

The inclusion of certain information society service providers is particularly interesting, perhaps signalling recognition of the importance of certain online functions in society today. But has the scope of 'market operators' been drawn too widely? For example, whilst a case could be made for placing enhanced security requirements on internet payment gateway operators, social network providers might well wonder why they are being asked to comply with the same standards being placed upon those in the energy and financial services sectors.

Another concern is the lack of certainty over which businesses will be affected. The examples of market operators under the Directive are described as 'non-exhaustive' and Member States may have different interpretations of these terms in practice. Furthermore, Member States must also impose the Chapter IV obligations on 'public administrations', which has not been defined at all. This lack of clarity creates an uncertain outlook for businesses and carries a real risk that the Directive will be applied inconsistently across the European Union.

See the tool below establish whether the Directive could apply to your organisation.

Too onerous?

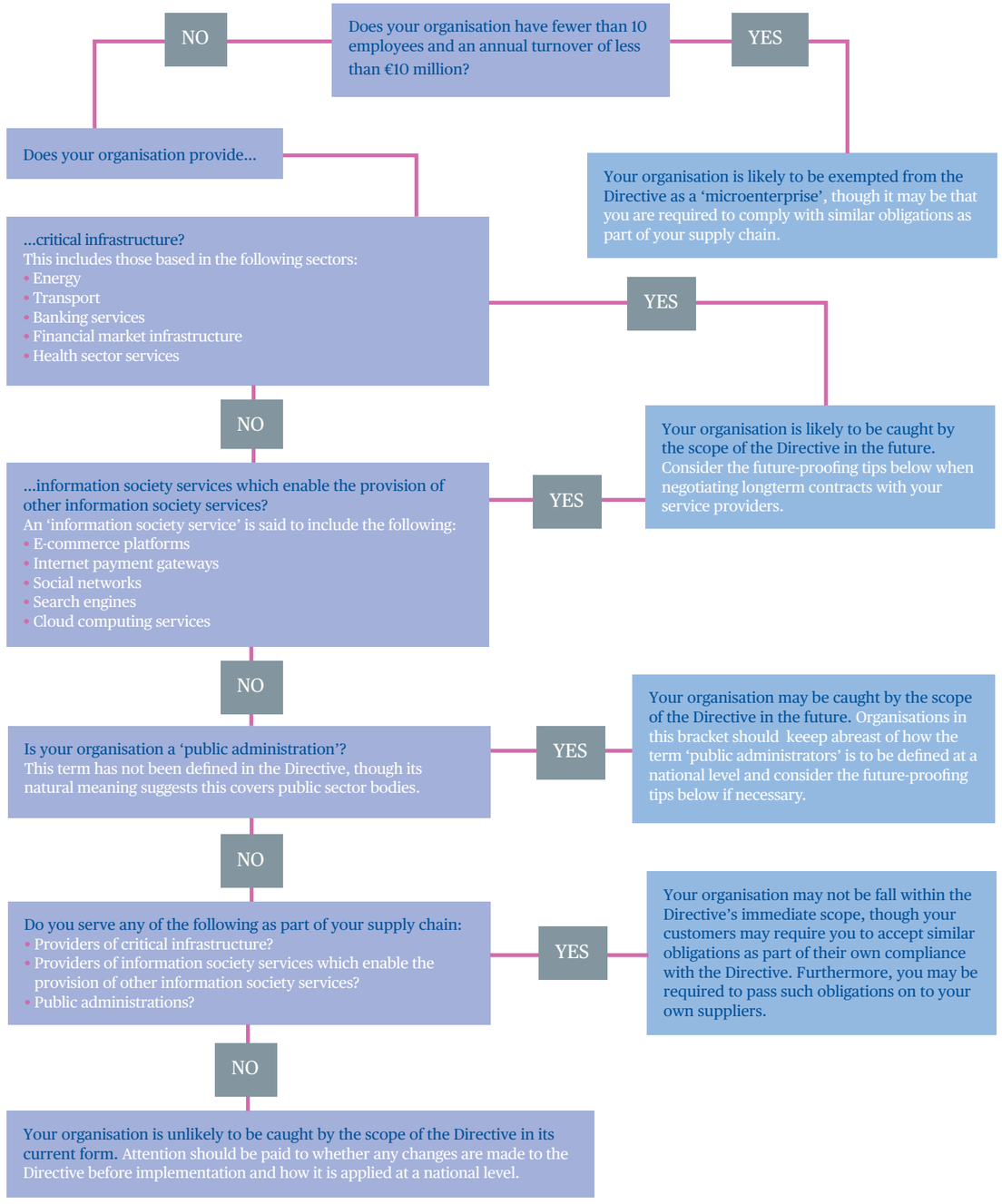
One cause for concern is that Chapter IV requires Member States to impose requirements that 'guarantee a level or security appropriate to the risk presented'. The impact this has on industry could potentially be quite significant - what level of investment and organisational effort would an organisation need to undertake to 'guarantee' its security?

Information sharing

As stated above, one of the aims of the Directive is to facilitate the exchange of information and early warnings amongst Member States. In parallel, the Directive asks Member States to impose notification and audit requirements at industry level. This raises a number of issues:

- Market operators and public administrations will be required to notify the NCA of any incidents that have a 'significant impact' on its core services. No further guidance has been offered on what sort of incident would trigger mandatory notification and this could lead to uncertainty in practice;
- In turn, the NCA may make such information publically available where it decides that it is 'in the public interest' to do so. The Chapter III provisions in the Directive suggest that such information could also be exchanged between NCAs at a European level. Businesses may be reluctant to notify their NCA of any incidents through fear that the information will be shared further or made publically available, particularly where its disclosure could result in bad publicity or breach of any confidentiality obligations that they owe to third parties; and
- The Directive proposes that NCAs are given broad powers to audit market operators and public administrations. As well as confidentiality concerns, businesses may also need to consider whether their commercial contracts allow them the freedom to facilitate such audits.

Flow chart diagram to determine the scope of the Cybersecurity Directive



Future-proofing tips:
When adopted, the Directive could have a significant impact on your existing commercial contracts. You may wish to consider the following tips prior to committing to any long-term commercial agreements with your suppliers:

- Tailor confidentiality clauses accordingly.
- Ensure sufficient audit rights are in place.
- Include appropriate 'change of law' provisions (i.e. requiring the supplier to comply with all current and future laws).
- Oblige the supplier to comply with your reasonable internal cybersecurity standards, as may be updated.
- Make sure that a sufficiently robust contract change procedure has been included.
- Include appropriate indemnities from the supplier, such as an indemnity against losses arising from breach of cybersecurity law and payment of regulatory fines.