HERBERT SMITH FREEHILLS

BATTENING DOWN THE CYBER HATCHES: EU COUNCIL APPROVES CYBER SECURITY DIRECTIVE

08 June 2016 | Europe
Legal Briefings

On 17 May 2016, the Council of Europe formally adopted the new Network and Information Security Directive (the so-called "**Cyber Security Directive**"), paving the way for final approval from the European Parliament.

As part of the Cyber Security Directive, Member States will be required to adopt a national 'NIS strategy' which will define strategic objectives and appropriate policy and regulatory measures in relation to cyber security. Member States will also be required to designate a national competent authority for the implementation and enforcement of the Directive, as well as Computer Security Incident Response Teams ("**CSIRTs**") responsible for handling incidents and risks and to promote swift and effective operational cooperation on specific cyber security incidents and sharing information about risks.

Critically for organisations, the Directive will also apply security and incident reporting obligations on two distinct categories of organisation, being: (i) operators of essential services; and (ii) digital service providers.

Operators of essential services will be required to adopt risk management practices and report major security incidents on their core services to the appropriate national authority or CSIRT. The original text of the Directive defined these operators broadly to include information service providers – internet payment gateways, social networks, search engines, cloud computing providers and app stores – and operators of critical infrastructure, such as electricity and gas suppliers, operators of oil and natural gas, air carriers, maritime carriers, railways, airports and ports, traffic management operators, banks, financial market infrastructure and health care providers. However, the final agreement between the European institutions provides that Member States will identify the operators in their jurisdiction to fall within the scope of the Directive, based on three criteria laid down in the text. These criteria are that:

- they provide a service that is essential for the maintenance of critical societal and/or economic activities;
- the provision of that service depends on network and information security; and
- an incident impacting the network and information security would have significant disruptive effects on the provision of those services.

Digital service providers are also subject to express security and notification requirements. Digital service providers are providers of online marketplaces, online search engines and cloud computing services, but hardware and software developers are excluded, as are social network providers. Digital service providers are required to take appropriate and proportionate technical and organisational measures, having regard to the state of the art, to manage the risks posed to the security of the network and information security used in the provision of service within the EU. They are also required to notify the competent authority or CSIRT without undue delay of any incident having a substantial impact on the provision of their service.

Organisations who are not operators of essential services or digital service providers may also notify the competent authority or CSIRT of any incidents but are not mandated to do so.

The text of the Cyber Security Directive will now have to be formally approved by the European Parliament. After that it will be published in the EU Official Journal and will officially enter into force. Member States will then have 21 months to implement the Cyber Security Directive into their national laws and six further months to identify operators of essential services in their jurisdiction.

For further details regarding the Cyber Security Directive, please click here.

However, cyber security is not just a regulatory compliance issue. There are a number of proactive and reactive steps that organisations should take in order to prepare for, and react to, a cyber attack.

From a proactive perspective, it is vital that organisations carry out the following five key steps:

- **Risk Assessment** - Carry out a comprehensive risk assessment to identify assets and risks.
- **Incident Management Strategy** - Establish effective incident management policies and processes, and keep them under review
- **Employee Education and Awareness** - Consider how to effectively embed risk management and cyber security within the organisation
- **Regulatory and Compliance Governance** - Pay attention to regulatory requirements, in particular cyber incident reporting requirements
- **Network and IT Security** - Take appropriate steps to ensure that networks and infrastructure are defended against external and internal attacks

From a reactive perspective, organisations will need to respond to a cyber incident in the following five key phases:

- **Detect** - Detecting a cyber incident is not always as easy as you would think
- **Assess** - The early assessment of a cyber attack is sometimes the most difficult step, with decisions needing to be made under considerable time pressure and on the basis of incomplete information
- **Contain** - Appropriate measures to contain a cyber attack will depend on the type of attack as well as the type of business in question
- **Investigate** - Use a legal team to manage any investigation in order to preserve legal privilege
- **Remediate and Review** - Reflect on the causes of the breach and remediate them so that the same attack cannot recur.

For further details regarding our Top Ten Tips for Businesses with respect to Cyber Security, please click here. This article first appeared in the January/February 2016 edition of PLC magazine - click here for the PLC Magazine homepage.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

NICK PANTLIN
PARTNER, LONDON

+44 20 7466 2570
Nick.Pantlin@hsf.com

DAVID COULLING
PARTNER, LONDON

+44 20 7466 2442
David.Coulling@hsf.com

MIRIAM EVERETT
PARTNER, LONDON

+44 20 7466 2378
Miriam.Everett@hsf.com

LEGAL NOTICE