ARE YOU KEEPING PACE WITH CYBER SECURITY RULES AND REGULATIONS?

Global
Legal Briefings

The issues surrounding cyber security and the broader concept of cyber-resilience are the focus of increased regulatory attention across the globe. At a national level, most countries do not have a single law dealing with cyber security. Instead, there is a patchwork of rules and regulations which have developed in response to the evolving cyber threat. Some of these apply to all organisations while industry-specific legislation is continuing to develop to govern the most at-risk sectors.

This lack of harmonisation makes it difficult to keep pace with regulatory and compliance obligations, especially for organisations that do business in a variety of jurisdictions.

In the last few years, we have seen a number of initiatives from legislators around the world. These include a **Cyber Security Executive Order in the US**, and a proposed **Cyber Security Directive in Europe**. However, the regulators freely acknowledge that a detailed prescriptive approach to regulation in this area will not work, given how quickly technology and the related threats evolve.

In essence, the regulators expect firms to demonstrate that they have robust cyber security defences in place. This will extend not only to ensuring that adequate preventative measures are established, but will also encompass crisis management planning and response processes to mitigate a cyber attack.

'ADEQUATE' CYBER SECURITY MEASURES

It is difficult to generalise as to what level of cyber security will be sufficient to meet an organisation's regulatory obligations. As with other types of systems and controls, much will depend on the scale and complexity of an organisation's business, the nature of the systems involved and the particular risks associated with their activities. For larger and more complex organisations, the interconnectivity of complex networks and IT systems, coupled with attempts to integrate legacy systems, or those inherited through acquisitions, means that such measures are frequently more challenging to implement in practice.

One way in which organisations can obtain some comfort that their cyber security measures are adequate to meet both industry standards and satisfy regulatory expectations would be to use a recognised framework. However, compliance with industry standards does not necessarily mean that you meet regulatory obligations, or that a successful cyber attack could not still occur.

In the UK, the Department for Business Innovation and Skills has developed a Cyber Essentials certification scheme in collaboration with cyber security experts and industry representatives. Although most suited to small and medium firms, Barclays' digital banking arm was amongst one of the first organisations to participate in the scheme.

The US National Institute of Standards and Technology's Cyber Security Framework, issued in 2014 is also assuming a higher international profile. The **Australian Securities and Investments Commission (ASIC)** views the NIST Cyber Security Framework as having "*particular relevance for our regulated population – specifically financial service providers that operate in a global environment, given the reach and dominance of US markets and the businesses operating within them*".

The **International Organization of Securities Commissions (IOSCO)** has also looked at cyber security in the context of market infrastructure and is consulting on guidance to enhance cyber resilience. The output may also be helpful to firms in assessing the strength of their own cyber security measures.

To sum up, when assessing what level of protection to apply to an organisation, the key is proportionality. In most jurisdictions, a strict regulatory approach to the requirements themselves will not be imposed. Instead, organisations are relied upon to know their business the best and be able to identify the areas of risk in order to implement suitable and adequate counter-measures.

Cyber security is not a “one size fits all” regime – board level executives will have to tailor their cyber security arrangements to suit their risk profile. In addition to regulatory and compliance obligations boards need to consider their third-party suppliers and most importantly their shareholder and customer expectations.

LEGAL NOTICE

The contents of this publication are for reference purposes only and may not be current as at the date of accessing this publication. They do not constitute legal advice and should not be relied upon as such. Specific legal advice about your specific circumstances should always be sought separately before taking any action based on this publication.
