June 21, 2019

IOSCO report underlines cyber-risk standards for financial services firms

Attorneys
Rosemarie Paul
Chris Stott
Rohan Massey
Edward R. McNicholas

Reflecting its ever-increasing importance on regulators' lists of priorities, the Board of International Organization of Securities Commissions ("IOSCO"), the global grouping of securities regulators, has (on 18 June) published a report that may act as a catalyst to further regulatory scrutiny of firms' cyber-risk arrangements.

The report highlights how several internationally recognised frameworks already in place (referred to as the "Core Standards"), which are considered to encapsulate best practice in this area, are being applied in practice and could be replicated in jurisdictions where they are not already reflected in regulators' rulebooks. IOSCO has chosen to focus on the Core Standards in the hope this will achieve greater consistency, rather than seek to implement new and/or additional cyber-standards.

The Core Standards consist of:

- the CPMI-IOSCO Guidance on cyber-resilience for Financial Market Infrastructures;
- the National Institute of Standards and Technology Framework for improving Critical Infrastructure Cybersecurity; and
- International Organization for Standardization 27000 series standards.

These are detailed frameworks which set out desired outcomes and principles-based and technical guidance for firms and authorities on preventing, responding to and mitigating the impact of cyber-related incidents. They are not prescriptive or mutually exclusive, and indeed IOSCO's report found that the majority of jurisdictions incorporate different elements of them flexibly into their national frameworks.

IOSCO examined how member jurisdictions are currently using the Core Standards, finding that, whilst they may not be expressly referenced in national regulatory arrangements, a majority of survey respondents indicated that their domestic regulations, guidance, and/or supervisory practices were either "generally consistent" or "entirely consistent" with one of the Core Standards. In terms of general awareness of cyber-risk, IOSCO's survey also found that cyber is widely recognised as one of the key risks facing firms but there is significant uncertainty in some jurisdictions about its particular characteristics and how responses to it should be differentiated from those for other risks. Some respondents also expressed uncertainty about where cyber-risk should be ranked as against others.

IOSCO has sought to address areas of uncertainty and promote best practice in relation to cyber-risk by suggesting a list of 15 questions for entities operating in the financial services sector. The questions are broadly grouped to raise awareness of cyber-risk and help regulators and firms understand how they may apply the Core Standards in relation to the identification of risks and vulnerabilities, detection of specific threats and response to/recovery from particular incidents. They are directed towards assisting regulators and firms with diagnosing weaknesses and applying the most apposite parts of the Core Standards to counter them.

The IOSCO report will not lead directly to enforcement action against firms or individuals. However, the IOSCO report does encourage regulators to consider their current cyber-standards in comparison with the Core Standards and use these as a basis to strengthen their regimes.