December 13, 2018

U.K. financial regulator flags deficiencies in firms' cyber practices

Attorneys
Rosemarie Paul
Rohan Massey
Edward Machin

A review of the U.K. asset management and wholesale banking sectors by the Financial Conduct Authority ("FCA") has found that regulated firms struggle to identify and respond to the specific cyber risks facing their businesses.

In a report released on Monday 10 December (the "Report"), the FCA detailed the findings of a multi-firm review it conducted in late 2017 and early 2018 of 20 firms varying in size, structure and business model. The firms surveyed had assets under management ranging from £15 billion to £500 billion and services ranging from boutique offerings to full-service models. The aim of the review was to help assess how firms oversaw and managed risk in this area, how they identified and mitigated risk and their capability to respond and recover from attacks.

Whilst acknowledging that the small sample size is not statistically significant, the Report makes clear that the FCA considers its findings will be relevant to all firms in the asset management and wholesale banking sectors. Given that the FCA is taking an increasingly aggressive approach to enforcement of cybersecurity incidents (see below), we advise that regulated firms pay close attention both to the Report and future developments in this area.

What does the Report say?

A full copy of the Report can be accessed here. Its key findings are as follows:

Most boards have limited familiarity with the cyber risks their organisations face

- Almost all of the board members and non-IT senior management interviewed told the FCA how difficult it is to fully understand and explain these specific risks. This challenge is compounded by the fact that most board members and non-executive directors lacked familiarity with, or specific technical expertise in, cybersecurity.
- Some firms have hired external parties to advise them on cybersecurity. Whilst endorsing this approach, the FCA cautioned against an over-reliance on such advisors, which it said could hinder the development of firms' in-house cyber awareness and abilities.

Risk and compliance functions have limited technical cyber expertise

- The FCA observed that a company's second line of defence — its risk and compliance functions — also had limited experience with cybersecurity, raising the prospect that such functions would be unable to challenge technically sophisticated first line business units.
- Firms that included the chief information security officer ("CISO") in their first line alongside or as part of their IT function appeared to show a significant difference in the level of knowledge between the first and second line functions.

Firms do not actively consider how to include cybersecurity in their broader approach to conduct risk

- Many firms in the wholesale banking sector — including those with robust conduct risk frameworks already in place — fail to join the dots between cyber and other conduct issues that may occur through cyber channels, such as market abuse and financial crime.
- Firms told the FCA that their most significant cyber risks related to "insiders", highlighting the importance of embedding a security culture throughout all aspects of the business.
- The firms interviewed mitigated the threat of insiders in various ways, including: improving logical access controls; classifying data according to its sensitivity, commercial value or other special characteristics; and training and awareness initiatives.

Why does the Report matter?

The Report comes amid a heightened focus on cybersecurity following a series of high-profile data breaches at UK multinationals and the introduction of the EU's General Data Protection Regulation, under which fines of up to two per cent of an organisation's annual worldwide turnover can be issued for failing to implement security measures to protect personal data.

Unsurprisingly, informational security is now firmly at the top of most boardroom agendas — as well as those of U.K., EU and international regulators. For example, in a report on global cyber reliance practices issued on 4 December 2018, the Basel Committee on Banking Supervision echoed several of the FCA's findings — including that (i) cyber resilience is not always clearly articulated across all technical and business lines, hampering their effectiveness; and (ii) there is a skills shortage for individuals with cyber expertise across industries and geographies.

Although firms and regulators are both navigating uncharted waters in relation to cyber compliance and enforcement, U.K. authorities have historically been willing to exercise their powers in this area. The FCA's predecessor, the Financial Services Authority, fined a number of financial services organisations for their data security failings, whilst the UK's data protection regulator, the Information Commissioner's Office, twice issued a £500,000 penalty — the maximum permitted under the previous legislative regime — in respect of personal data breaches.

Most notably, the FCA in October 2018 fined Tesco Personal Finance plc £16.4 million for its failings in relation to a cyber attack in November 2016. In announcing the fine, the FCA's first for cyber fraud, the regulator said:

- A financial institution's board has the ultimate responsibility for ensuring that its cyber crime controls are designed to meet standards of resilience.
- The board must set an appropriate cyber crime risk appetite and ensure that its institution's controls are designed to anticipate and reduce the risk of a successful attack.
- Where an attack is successful, the board should ensure that its institution's response plans are clear, well-designed and that the institution recovers quickly from the incident.

Conclusion

The Report's focus on board-level ownership of and responsibility for their firm's approach to cybersecurity is not new. However, given the FCA's stated position is that many organisations have work to do in implementing the technical and organisational measures required to defend against cyber risks, regulated firms and their boards should ensure that these measures are put in place as a matter of priority for 2019.