April 1, 2020

FCA's Head of Technology, Resilience and Cyber outlines expectations on cyber resilience and security

Attorneys
Rosemarie Paul
Rohan Massey
Tom Jackson

In a recent episode of the Financial Conduct Authority's ("FCA") "Inside FCA" podcast, Robin Jones – the FCA's Head of Technology, Resilience and Cyber – provided insights on the most pressing cyberthreats firms currently are facing, as well as some of the emerging threats he believes firms increasingly will face in the future.

Although the podcast preceded the current crisis, the issues discussed are particularly pertinent at this time, with COVID-19 causing significant disruption to the manner in which firms are operating and in particular the extent to which employees are working remotely, and consumers are relying on on-line services. The FCA recently published an information page for firms on COVID-19 responses, in which it set out its expectation that all firms should have contingency plans to deal with such major events.

Key points arising from the podcast include the following:

- **Cybersecurity measures must keep pace with technological advances.** Rapid development and innovation in the financial services sector brings clear advantages to customers, but also give rise to new cyberthreats and vulnerabilities. Firms should ensure cyber security measures keep pace with technological development, and that they manage communications with customers effectively in the event new and innovative technology does not meet customer expectations. As technology develops and becomes more complex, the potential for something to go wrong increases and systems may become more vulnerable to attackers. Complexity will always be an area that cyber criminals will look to exploit.
- **Continued focus on people as a significant cybersecurity threat.** Mr. Jones sees people as an important area of cyber vulnerability. People design, build, test and use technology, and an incredibly secure system can become vulnerable if its users are fooled into compromising security by divulging confidential or sensitive information. By giving customers more technology and means to access financial services, firms also have provided cyber criminals with a greater variety of routes to access customers and exploit weaknesses in cyber security.
- **The FCA increasingly is focusing on firms' cyber resilience.** It is asking firms to identify their key services and, hence, where their business needs to be most resilient. A firm should shift its perspective away from thinking about how it can stop issues arising and toward greater consideration of the steps it can take in the event of a cyber-incident, how services can continue to be provided, and how to communicate effectively with stakeholders.
- **Firms of all sizes should also focus on their "cyber hygiene".** This means considering who can access systems and data, how such access is managed and monitored, and how systems can be updated or "patched" in a manner that does not cause interruption to key services. Firms should focus on leadership and setting an appropriate "tone at the top" to ensure all employees, whether junior or senior, take cybersecurity matters seriously. In developing a robust security culture, a firm should test its staff (for example, by sending fake phishing emails)

and provide training and guidance on areas such as managing personal information online, including through use of social media. Although smaller firms may have fewer systems and a reduced degree of complexity, the same principles apply – such firms should focus on "cyber basics", particularly around areas such as phishing emails, which are one of the most frequent threats faced by smaller enterprises.

- **Increased emphasis on "security by design".** Firms should ensure cybersecurity considerations are built into a system's framework from the outset. The FCA perceives cybersecurity as one of the areas where firms are weak, owing in part to the fact that firms frequently change and update their systems, which often causes those systems to work less effectively. According to Mr. Jones, firms often fail adequately to keep customers updated, informed, and manage cyber issues appropriately.
- **A changing landscape of future threats.** Mr. Jones believes people will continue to be one of the biggest areas of cyber vulnerability. In particular, increased use and proliferation of mobile devices and remote working requires firms to shift their focus away from security of office-based systems. Mr. Jones also flagged the advent of quantum computing – which has the potential to render many existing security measures obsolete – as a significant future challenge.

It is clear that operational resilience remains a key priority for regulators, and the issue has been brought into sharp focus by the current period of profound uncertainty. The COVID-19 pandemic has emerged at a crucial stage in the development of a regulatory framework for operational resilience, with responses to the FCA, PRA and BoE's consultation papers on the proposed operational resilience framework now extended to 1 October 2020. COVID-19 thus not only provides a stern test of the operational resilience measures firms currently have in place, but likely will also shape the regulatory framework governing such matters for years to come.