Cyber-resilience—a repeated regulatory message

MAY 8, 2017

An expectation that regulated financial services firms be 'cyber-resilient' should not cause any surprise. Cyber-crime and data breaches represent major risks for business generally. Comparatively, that risk is not mitigated by the standards of British employees, who have been found to be particularly ineffective at protecting their data and devices.[1] Accordingly, cyber-crime has the potential to be profoundly destabilizing, as well as costly, to the UK financial services sector.

However, the framework against which the expectation of cyber-resilience translates into tangible and measurable obligations is not substantially developed. Two recent FCA public announcements provide some insight into the Regulator's approach to cyber security, and indicate the direction and shape of regulatory change. The FCA released its Business Plan for 2017/2018 on 18 April.[2] The document sets out the FCA's priorities. 'Technological change and resilience' is one of six cross-sector priorities listed. The following week, on 24 April, the FCA's acting COO (Nausicaa Delfas) delivered a speech at the Financial Information Security Network, titled "Expect the Unexpected - cyber security - 2017 and beyond".[3] Ms. Delfas reviewed the landscape of cybercrime risk, before proposing ways of managing it.

Unsurprisingly cyber security is a growing priority for the FCA, and is therefore likely to be within the cross-hairs of its Enforcement Division. Accordingly, although these public statements do not represent rules or formal guidance, firms should ensure that the principles espoused are carefully considered and, where applicable, properly implemented. Below we have distilled five key messages from the announcements.

1) Prevent, detect, recover, respond

Although historically the focus has been on prevention, the FCA has emphasised that firms must address their capacity to detect, recover and respond to any attack. Firms should have adequate and appropriate systems which allow them to continue functioning in the event of an unforeseen interruption. One key feature of a firm's capacity to recover effectively concerns its back-up strategy, the importance of which is underlined by the risk posed by Ransomware. Ms. Delfas stated that the FCA expect firms to maintain online and offline backups".[4]

Moreover, the Regulator expects firms to ensure that both consumers and markets are, where

appropriate, informed about material breaches in timely fashion. An appropriate response is likely to be delayed where firms have not formulated and implemented, ahead of time, a clear strategy and chain of responsibility.

The need for firms to defend and respond to cyber-attacks, and do so quickly and effectively, is repeated in the FCA's Business Plan.

2) Getting the basics right: the majority of crystalised risk could be easily avoided

For all the apparent complexity of cyber-crime, several recent studies have underscored a simple truth: most breaches would be prevented by the adoption of basic measures. Ms. Delfas referenced a 2016 data breach investigations report. The report detailed the findings of a wide-ranging analysis of various data breaches and security incidents, from across sixty-one countries. The report found that ten vulnerabilities accounted for 85% of successful breaches. Moreover, the majority of the vulnerabilities exploited during attacks were well-known and easily fixed.

The FCA clearly believes that the report's findings are reflective of the risks posed by UK financial services firms. On that basis Ms. Delfas stressed the importance for firms to get the basics right. She cited the statistic that, properly implemented, the ten steps to cyber security, published by the National Cyber Security Centre,[5] would eliminate 80% of the cyber threats which firms are struggling to manage. Furthermore, she urges firms to carry out robust comprehensive risk assessments focused on the impact of a Distributed Denial of Service (DDoS) attacks on their system.

3) Third party oversight

One recurring theme in the FCA's Business Plan, reflective of regulatory practice more generally, concerns the duty on firms to monitor and oversee the risks faced by third party service providers. By outsourcing its IT systems or processes a firm does not necessarily escape regulatory responsibility for any resulting failures attributed to cyber-attacks. This point was stressed by Ms. Delfas in a previous speech made in September last year.[6] Firms are expected to perform appropriate and adequate oversight of third party service providers. Similarly, the Business Plan identifies issues associated with oversight and control of increasingly complex chains of third party relationships in the context of Fintech companies. Firms should be conscious that Fintech companies may not properly understand the scope of regulation or its impact on their business model.

4) Fostering a "secure" culture

The promotion and embedment of good regulatory culture in firms has been an FCA focal area for some time. It will come as little surprise that Ms. Delfas' speech echoed that expectation in the context of cyber-security. The mere production and distribution of a cyber-security policy may not meet the standards expected by the Regulator. Firms must make continual efforts to promote and strengthen good behavior amongst its staff. Ms. Delfas encouraged firms to take staff "on a journey". She elaborated on this concept in slightly less ambiguous terms, suggesting that firms circulate fake phishing emails. Depending on their response staff should be educated or rewarded accordingly. A good example of this practice comes from the US Federal Government. Its

Department of Home Security is reported to have emailed its employees, offering free tickets to an NFL match. Anyone who clicked on the attached link was subject to a mandatory cyber-security course.[7]

An obligation to foster good "culture" does however present regulatory challenges. In her speech Ms. Delfas alluded to the problem posed in measuring a firm's culture, which she concedes is a "qualitative and intangible concept". However, she articulated a mechanism for calibrating the culture of a firm:

> *"by aggregating the outcomes of ethical phishing exercises, red team tests, senior leadership exercises, staff awareness events and information security training, we can begin to gather baseline metrics against which to track improvement. By tracking improvement, we can begin to make tangible steps to improve our cultural attitude towards security and start to tackle the more difficult challenges emanating from within our organisations."*

A failure to demonstrate marked improvements in these baseline metrics—or simply an abject failure to meet acceptable standards—could result in an enforcement action against the firm.

Non-executive directors also have a responsibility to promote a coherent and effective cyber culture. Ms. Delfas suggested that NEDs, should satisfy themselves that their companies are managing cyber risk effectively.

5) Information sharing

The FCA has seen a sharp increase in the number of cyber-attacks reported to the FCA: from 5 in 2014, increasing to 89 last year. Ms. Delfas rightly queries whether this surge can be attributed to greater detection and reporting, rather than an increase in the prevalence of attacks. Notwithstanding this trend, outside of financial institutions which are considered of critical or systemic importance, the FCA has noticed a lack of cyber information being shared by firms. Information exchange in cyber-security will play a major role in the FCA fulfilling it public functions in the future. In recognition of this, the FCA has established several Cyber Coordination Groups to better understand how threats differ across the various sectors of the industry. Through information sharing the FCA hopes to improve the resilience of the sectors it regulates.

These comments are not merely an expression of encouragement, but should be read as an articulation of firms' regulatory obligations. Under Principle of Business 11 (PRIN 11) firms "*must deal with its regulators in an open and cooperative way, and must disclose …appropriately anything relating to the firm of which that regulator would reasonably expect notice.*" Public announcements like Ms. Delfas' speech signal to firms that the FCA expects to be notified of cyber information, even if it is not of direct significance to the supervision of the firm itself. During her speech in September Ms. Delfas commented, "*I cannot emphasise enough how important information sharing is to identifying and tackling patterns of attack*". Firms should assume therefore that attempted cyber breaches—however efficiently they were detected or responded to—may trigger a disclosure obligation.

Conclusion

Although not formal guidance, public announcements by the FCA, in any form, signal the standards it expects firms, and their managers, to meet when implementing cyber security. As such, these announcements typically foreshadow the Regulator's enforcement priorities. It may take some time before the FCA's expectations are considered adequately developed and rehearsed to ground any enforcement action. However, good practice and culture can take a significant time to foster and embed. These announcements may prompt firms to review their current procedures and test the standards being applied by their employees.

---

[1] One study shows that British workers came 9th out of 10 countries for failing to protect their data and devices, see www.ft.com/content/e75d9c96-eec9-11e6-ba01-119a44939bb6.

[2] www.fca.org.uk/publication/business-plans/business-plan-2017-18.pdf.

[3] www.fca.org.uk/news/speeches/expect-unexpected-cyber-security-2017-and-beyond.

[4] It is worth noting that this standard had previously been emphasized during a similar speech delivered Ms. Delfas in September of last year, available at www.fca.org.uk/news/speeches/our-approach-cyber-security-financial-services-firms.

[5] These steps were issued as guidance by the National Cyber Security Centre, and can be found at www.ncsc.gov.uk/guidance/10-steps-cyber-security.

[6] www.fca.org.uk/news/speeches/our-approach-cyber-security-financial-services-firms.

[7] See www.ft.com/content/e75d9c96-eec9-11e6-ba01-119a44939bb6.