COLLAS CRILL

Cyber security: A time for increased vigilance?

APRIL 2022

In this article we explore the need for firms to consider increasing their cyber security vigilance, and how they might achieve that.

Cyber security from a global perspective

While poor cyber security has been high on the list of risks posed to financial services businesses for some time now, the war in Ukraine has heightened firms' cyber risk exposure. Globally there is a real awareness that cyber crime is developing at an incredibly fast pace, and the war in Ukraine has highlighted that not only is there an increased risk in criminal cyber-attacks, but also that the threat of state-sponsored cyber attacks is at its highest level ever.

US President Joe Biden recently commented at a Business Roundtable meeting with CEOs of the largest US corporations that there is "evolving intelligence that the Russian government is exploring options for potential cyber attacks", urging the U.S. private sector to "harden their cyber defence immediately". Furthermore, the UK National Cyber Security Centre (**NCSC**) has supported this call for increased cyber security precautions.

A Guernsey perspective

In light of "the deteriorating international situation" on 24 February 2022 the local regulator, the Guernsey Financial Services Commission (**GFSC**), issued a request for all firms to check that they are familiar with the Cyber Security Rules and Guidance (the **Rules**), which came into force on 8 February 2021, noting that firms need to ensure that they:

- have appropriate cyber security software in place;
- implement IT systems updates in a timely manner; and
- encourage their staff to exercise caution, by not clicking on or opening unfamiliar links in emails or on websites.

This may seem like a general request, but the devil in is in the detail and firms should take this opportunity to comprehensively review the appropriateness of their cyber security framework, in light of the enhanced risks posed.

The Rules are based, and focus on internationally recognised cyber security principles, being to:

- identify;
- protect;
- detect;
- respond; and

- recover.

Firms must be able to evidence that the Rules have been considered and implemented in accordance with the size, nature and complexity of the business. Furthermore, firms "are required to have robust policies, procedures and controls in place to identify, assess and manage cyber security risks on an on-going basis consistent with the minimum licensing requirements" and these should reflect the Rules, as well as consider the guidance included throughout.

It's important to note that where a firm has outsourced large portions of their operations, the board of the firm is still responsible for the oversight of the services, and for compliance with the Rules.

Firms will already have a cyber security framework and policies, procedures and controls in place. However this recent request provides an opportunity for firms to conduct a review, in light of the recent changes to the cyber risk landscape, and in line with the Rules' requirement, to review all relevant measures adopted, in response to an "identified cyber security event". While there is little that can be done to influence cyber threat levels, the focus should be on each firm's vulnerability to attack.

The NCSC recently published a useful guide on actions that firms can take. The guide focuses on ensuring that the fundamentals of cyber security are in place and functioning correctly, which include reviewing the technical, people, administrative and governance controls such as:

- system patching;
- internal and third party access controls;
- antivirus/Firewall updates;
- cyber security logging and monitoring;
- backups;
- incident and Response plans;
- phishing response awareness of staff; and
- briefing any wider organisation.

What should boards consider?

Cyber risk should be treated like any other risk identified by the firm, and as such a review of cyber risk should follow any agreed risk review protocols.

Given the request from the GFSC, boards should be looking to undertake a review of their cyber security framework to ensure that they are comfortable the framework appropriately addresses the firm's current cyber risk landscape, and its defence, while adhering to the Rules. In doing so boards may wish to consider the following:

- Engaging with the relevant divisions and personnel, such as the Chief Information Security Officer (**CISO**), IT specialists, Compliance, Risk and Operations to determine the level of increased cyber risk posed to the business.

- Ensuring that staff are aware of the heightened cyber risk, and reminding them of the appropriate policies and procedures, in particular payment instructions.
- Requesting analysis from the relevant divisions and personnel of the cyber risks, potential impact and what defences can be put in place to mitigate these risks, while keeping in mind the guidance provided in the Rules and other relevant bodies, such as the NCSC.
- Determining the resourcing required in respect of any resultant recommendations from the analysis. This may also include consideration of "less critical" system updates being delayed to allow for prioritising more critical work.
- Taking pro-active steps in overseeing that any agreed plan of action is implemented in a timely manner, in order to address any gaps identified in the analysis, and crucially ensuring they formally evidence any consideration and decision making.
- Ensure any Incident and Response plans are up to date, accurate and fit for purpose.
- Determine whether there is a need for increased reporting around cyber security, given the recently increased risks, in order to ensure the board is kept up to date on any developments within the cyber security arena and potential impacts on their business.
- Update policies, procedures and controls to reflect any necessary changes brought about as a result of this exercise.

While considering the above, it is prudent to note that where IT systems and solutions are provided as part of a wider group, the local board should ensure that it is appropriately engaged and kept fully informed of any action taken from a group perspective to address the escalating cyber security risks.

In such instances, the firm should ensure that it is able to clearly evidence engagement and consideration of how the wider group is addressing the increased cyber risks posed to the business. It should formally document what is being conducted at a group level, but also document an assessment that it is suitable from a local perspective, and how it can gain comfort that cyber risks are sufficiently addressed and that the firm are adhering to the Rules.

COLLAS CRILL

For more information please contact:

Sandra Lawrence

Head of Compliance | Guernsey

t: +44 (0) 1481 734808 | **e:** sandra.lawrence@collascrill.com