167 Fleet Street, London EC4A 2EA, UK
+44 (0)20 7822 8380
info@aima.org

aima.org

Financial Stability Board
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Submitted via email to CIRR@fsb.org

20 July 2020

Dear Sir or Madam,

Re: AIMA's Response to the FSB's Consultation on Effective Practices for Cyber Incident Response and Recovery

The Alternative Investment Management Association Limited (AIMA)[1] appreciates the opportunity to respond to the Financial Stability Board (FSB)'s consultation[2] on developing a toolkit for financial institutions on effective practices to respond to and recover from a cyber incident.

We previously responded to the FSB's industry survey[3] on Cyber Incident Response and Recovery (CIRR), where we commented on the challenges around the complex cyber standards landscape, increased reliance on third-party service providers, e.g., cloud services, as well as the perceived communications and cyber security capability gap.

In recent years, cyber security has increasingly become a top global risk for businesses, with regulators and policymakers rightly paying increased attention to how financial institutions manage their cyber security risk.

[1] AIMA, the Alternative Investment Management Association, is the global representative of the alternative investment industry, with around 2,000 corporate members in over 60 countries. AIMA's fund manager members collectively manage more than $2 trillion in hedge fund and private credit assets. AIMA draws upon the expertise and diversity of its membership to provide leadership in industry initiatives such as advocacy, policy and regulatory engagement, educational programmes and sound practice guides. AIMA works to raise media and public awareness of the value of the industry. AIMA set up the Alternative Credit Council (ACC) to help firms focused in the private credit and direct lending space. The ACC currently represents over 170 members that manage $400 billion of private credit assets globally. AIMA is committed to developing skills and education standards and is a co-founder of the Chartered Alternative Investment Analyst designation (CAIA) – the first and only specialised educational standard for alternative investment specialists. AIMA is governed by its Council (Board of Directors). For further information, please visit AIMA's website, www.aima.org.

[2] https://www.fsb.org/wp-content/uploads/P200420-1.pdf.

[3] https://www.fsb.org/2019/07/cyber-incident-response-and-recovery-survey-of-industry-practices/.

We agree with the FSB's statement that a major cyber incident, if not properly contained, could seriously disrupt financial systems and an appropriate and effective cyber security programme by firms in the financial ecosystem is vital to limiting any related financial stability risks. Therefore, we fully support the FSB in its development of a toolkit for effective practices that aims to provide guidance to firms in their cyber security planning activities.

Following our response last year to the FSB's industry survey, we would like to focus our response to this FSB consultation on the following areas:

1. Proportionality

We would encourage the FSB and public authorities to apply the principle of proportionality when developing any new cyber-related practices or rules for both the financial services subsectors, e.g., banks, insurers and asset managers, and also within each subsector, taking into account the specific needs arising for specific categories of financial institutions, such as their business models, size and risk profiles.

We would support an approach whereby any proposed cyber security practices are aligned to the type of institutions. For example, larger and systemic institutions might anticipate being subject to more or more complex cyber-related requirements, while for smaller institutions these requirements could be less complex. Any proposed practices should not equally affect all financial institutions, as new practices or requirements should be calibrated to capture the major cyber incidents. For instance, some practices would be more relevant for significant financial institutions and impact less on smaller entities with fewer financial stability risks.

2. Principles and risk-based approach

Overly prescriptive and process-driven practices may be inappropriate at some financial institutions where being fleet of foot is essential when responding to a cyber incident. Smaller institutions can more easily achieve the same level of protection without the same expense in time and resources required for layer upon layer of security. With this in mind, we support a principles and risk-based approach to regulation and supervision around financial institutions' cyber security. Providing guidance to firms will be a useful tool in the development of their own CIRR activities taking into account their own business models, size and risk profiles.

3. Lessons learnt from the COVID-19 pandemic and related cyber activity

The experience of the COVID-19 pandemic has rightly increased attention by public authorities on cyber activity with a significant rise in COVID-19 related cyber threats. The focus areas of attackers have been on phishing scams targeting people's anxieties around the virus and hacks that exploit IT vulnerabilities associated with the hastened remote working roll-out.

Therefore, key areas of focus relating to cyber security for investment managers during the COVID-19 pandemic include appropriate remote access solutions, remote work policies and access controls, and suitable home office set up. Cyber security essentials that have been implemented by several of our members to safeguard onsite and remote working include:

- Simulated phishing scams and online training for employees

- Security Information and Event Management (SIEM) software and Dark Web Monitoring for a layered approach
- Home network security best practices:
    - Web filtering on remote networks
    - Firewalls for Company segment
- Multi-Factor Authentication (MFA) on all systems
- Separate/strong passwords
- WiFi management

Knowing that we cannot live without the digital component of the economy and as firms potentially move to a more permanent remote working environment, there is an increased sense of urgency that enhanced cyber security planning is necessary. Our members understand that cyber security and digital operational resilience are essential to their business models moving forward.

4. Role of authorities in supporting firms' cyber incident activities

Public authorities have a very important role to play in helping businesses stay on the front foot against future cyber attacks. Crucially, authorities must establish relationships with the private sector and provide early warning alerts and dissemination of information about cyber risks and incidents. They can also support firms with their CIRR activities by producing detailed reports on incident notifications to increase awareness and they must have in place the appropriate processes to ensure cross-border co-operation where incidents affect more than one country.

Finally, we often hear that employers struggle to recruit individuals with the required cyber security skills to lead an organisation's cyber security programme. Governments and relevant partners should work collaboratively to address the cyber security capability gap to ensure that firms have the cyber security capability they need to maintain resilience to increasing cyber threats. For example, this could include embedding cyber security and digital skills as an integral part of relevant courses within the education system. Everyone studying computer science, technology or digital skills must learn the fundamentals of cyber security. We appreciate that at the same time employers also have a responsibility to clearly articulate their needs, as well as train and develop employees' awareness and understanding of cyber threats. Overcoming the cyber security capability gap will require government and industry to work effectively together.

AIMA's Cyber Security Guide to Sound Practices

We do not believe that there is a one-size fits all solution to firms' CIRR planning. Each individual financial institution's programme must be appropriate to their business model, size and risk profile. Simply increasing cyber-defence expenditure is not always the most effective solution to managing cyber risk. AIMA has made available for its members in the investment management

industry its latest edition of a *Guide to Sound Practices for Cyber Security*[4]. The Guide runs through material considerations in the wider cyber debate to enable investment managers to have informed internal discussions to put in place a strategy to deal with a cyber incident.

The Guide is not intended to be the solution to all investment managers' cyber security issues. It is predominantly designed to frame the principles of the debate rather than directing it. The Guide seeks to enable those responsible for the implementation of a cyber security programme to fully understand the range of problems as well as to consider more sensibly what is and what is not applicable to them.

For further information or if you would be interested in seeing a copy of our *Guide to Sound Practices for Cyber Security,* please contact James Delaney, Director of Asset Management Regulation (jdelaney@aima.org).

Yours faithfully,

Jiří Król
Deputy CEO, Global Head of Government Affairs
AIMA

[4] AIMA's Guide to Sound Practices for Cyber Security; published in November 2019. Available to AIMA members at: https://www.aima.org/sound-practices/cyber-security-resources.html.