Jersey Financial Services Commission

22 February 2016

Dear Chief Executive

Cyber-security

I am writing to draw your attention to the growing importance of cyber-security arrangements and the Commission's expectations of registered persons in this regard.

The frequency, sophistication and impact of cyber-attacks is increasing. Over recent years it has become clear that most businesses and organisations are potentially vulnerable to an attack. The Commission itself is not immune to this risk. We recognise our responsibility to protect the information we hold. We take cyber-security very seriously and we have a robust approach to understanding and managing this risk. We cannot guarantee that we will not be the subject of an attack, but we do all that we can to minimise any risk and impact.

The financial services sector is an attractive target for cyber-attacks and therefore I expect that your business will already be aware of the potential effect such an attack would have on you and your clients. As recent events have illustrated, the impact of a successful attack can be significant. Common risks involve data / information theft, misappropriation of client assets and reputational damage. These all carry financial costs, which may be significant and may also result in breaches of the law and / or, for registered persons, regulatory requirements.

Given the potential impact on businesses, the public and the reputation of Jersey, we are keen to ensure that registered persons have appropriate cyber-security measures in place. To assist with this, we have identified a number of resources that are likely to assist with identifying and managing these risks. We have provided a brief description of these resources in Appendix 1 of this letter. Please note this list represents only some of the resources that are available; we consider it a good level of practical guidance for firms.

In taking this approach (as opposed to developing our own principles and / or guidance), we have not incurred the cost of establishing an Industry-focussed cyber-security resource. However that does limit the guidance that we can provide to registered persons. Whilst our supervisory staff are able to discuss regulatory requirements and risk mitigation considerations in general, they are not experts in cyber-security or the specific cyber-crime threats faced by your business.

We expect that registered persons will take appropriate steps to properly manage their cyber-security arrangements. Nevertheless, I would stress that, as with other operational risks, this management will be subject to the relevant Codes of Practice. I would also highlight that we consider that the growing level of threat will justify increased monitoring in the future of how registered persons are assessing and mitigating the risks to their business.

Existing cyber-security obligations under the Codes of Practice

The Codes of Practice differ according to the type of business conducted by the registered person, but we have identified some common themes that relate to cyber-security.

The core obligation covering cyber-security arrangements is Principle 3 of the Codes of Practice which, in most cases, states that "a registered person must organise and control its affairs effectively for the proper performance of its business activities and be able to demonstrate the existence of adequate risk management systems". The Codes of Practice also provide additional guidance on the interpretation of this Principle. For example, the following areas are typically covered:

- Corporate Governance – The need to assess the risks present in the registered person's business, to document those risks and the ways in which they are monitored and controlled.
- Internal Systems and Controls – These vary significantly amongst licence types, but in many cases include one or more of the following:
  - The business and affairs of a registered person must be adequately monitored and controlled at senior management and board level
  - The requirement to have adequate business resumption, disaster recovery and contingency arrangements in place, and tested at appropriate intervals
  - Management is able to properly guard against involvement in financial crime
  - The assets of the registered person are safeguarded and the liabilities controlled through measures designed to minimise the risk of loss from irregularities, error and fraud, and to identify any such occurrences promptly.
- Record Keeping – In most cases the following obligations apply as a minimum:
  - A registered person must ensure that they have appropriate record keeping arrangements for compliance with the applicable laws, Orders and regulatory requirements
  - A registered person must have a clearly documented policy and procedure regarding record retention that includes a periodic review of the accessibility and condition of paper and electronic records, and adequate safekeeping of those records.

It is important to note that these requirements are a summary of the existing obligations that apply to most registered persons. Some registered persons will be subject to different or additional requirements, and each registered person is expected to understand exactly what obligations they are required to comply with.

In the context of cyber-security, these requirements will typically mean that, as a minimum:

- A registered person should understand (and document) the risk of a cyber-attack on their business and take appropriate documented measures to mitigate this risk; the level and type of risk mitigation should be appropriate and proportionate to the type, potential impact and likelihood of the risks identified
- The registered person should have in place appropriate contingency arrangements that they can deploy in the event of a cyber-attack, for example maintaining service levels for clients or informing relevant parties about the attack and its impact

- A registered person should keep these matters under review and test their effectiveness at appropriate intervals
- Boards of Directors (or equivalent) of registered persons will take overall responsibility for ensuring that their firm adequately addresses cyber-security risks.

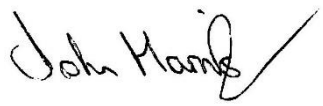
It is important to note that cyber-security risks can often result from relationships with third parties. We expect registered persons to take into account these associated risks in their risk assessment and where a contract with a third party is entered into.

These obligations are broadly consistent with international best practice on cyber-security, which involves identifying the risks, protecting key systems / information, detecting a cyber-security event, responding to an event (e.g. analysing the impact of the event and communicating with persons that may be affected) and recovering (e.g. restoring damaged capabilities). The importance of keeping up to date with, and sharing information on, threat-intelligence is also increasingly recognised as a key component of an effective cyber-security programme.

It is also worth reminding registered persons that, in accordance with the Principles set out in the Codes of Practice, they will typically need to notify us about a cyber-attack where such an attack might reasonably be expected to affect its registration or be in the interests of its clients/investors to disclose.

Should you have any queries regarding this letter, please feel free to contact your Supervision Manager at the Commission.

Yours sincerely,



John Harris
Director General

Appendix 1: Useful materials for managing cyber-security risks

A wide range of resources are available to firms in order to help them identify and manage their cyber-security risks. Here is a brief explanation of, and link to, a small number of particularly useful resources. This is only a small selection of the resources available in the public domain.

Firms need not rigidly apply any of the approaches referenced, but should at least be aware of the resources that are likely to be appropriate to them and consider whether they are suitable to their business.

UK cyber-essentials: A small number of fundamental mitigations that will stop the majority of internet based cyber-attacks against a firm's IT system. This is likely to be a core resource that is appropriate to most registered persons, especially smaller and medium sized enterprises. https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

The US National Institute of Standards & Technology's "Framework for Improving Critical Infrastructure": A detailed methodology for understanding risks and designing appropriate mitigation and control mechanisms. http://www.nist.gov/cyberframework/

The Central Bank of Ireland thematic review results: A list of best practices from Central Bank's thematic review of cyber-security arrangements in the investment firm and funds services industry. A list of questions that the Central Bank will typically pose prior to conducting an assessment: https://www.centralbank.ie/regulation/industry-sectors/investment-firms/mifid-firms/Documents/Industry%20Letter%20-%20Thematic%20Review%20of%20Cyber-Security%20and%20Operational%20Risk.pdf

The Hedge Fund Standards Board cyber-security toolbox: A number of practical approaches to identify and manage risk. It also contains links to a number of other useful cyber-security resources. Aimed specifically at hedge funds, but useful to a range of other entities. http://www.hfsb.org/sites/10377/files/cybersecurity_hfsb_toolbox_.pdf

JFSC thematic review: A themed assessment of information security in Jersey banks in 2011 identifying a number of good and poor practices: http://www.jerseyfsc.org/pdf/2011_Information_Security_Summary_Findings_March_2012.pdf

ISO standards: The International Standards Organisation has developed standards on information security (ISO 27001) and cyber-security (ISO 27032): http://www.iso.org/iso/home.html