Guernsey Financial Services Commission

Cyber Security – Regulatory Guidance

The Commission wishes to impress on firms the need for them to ensure that they take their responsibilities in respect of cyber security, seriously. Firms are reminded of their obligation to keep the Commission informed of matters involving financial crime and other serious operational problems. Any serious or significant incident involving data loss, financial loss or denial of service type attacks, whether actual or prevented, should be reported to the Commission in a timely manner.

The ability for firms to provide a secure and uninterrupted service should form an important part of their operational risk considerations. The increasing frequency and sophistication of cyber-attacks means that this is something which requires constant monitoring. Firms not only need to build defensive resilience to such attacks but also need to have the capability to recover quickly from the impact of a successful breach.

There is a considerable amount of professional guidance available on this subject. There is no regulatory obligation to follow the guidance contained in the links below but they do provide some very helpful practical assistance:

Centre for the Protection of National Infrastructure - http://www.cpni.gov.uk/advice/cyber/

CERT-UK - https://www.cert.gov.uk/resources/best-practices/

GCHQ – http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/Relaunch-10-Steps-to-Cyber-Security.aspx