JUNE 2021

UPDATE

Guernsey Cyber Security Rules and Guidance

Update prepared by Helen Wyatt (Guernsey) and Alasdair McKenzie (Guernsey)

Following a two-year consultation, the Guernsey Financial Services Commission (the **Commission**) has published the final form Cyber Security Rules (the **Cyber Security Rules**) and accompanying guidance under Guernsey's principal regulatory laws. The Cyber Security Rules have direct application to all persons licensed under these regulatory laws (**Licensees**). The accompanying guidance (the **Guidance**) provides the boards of Licensees (the **Board**) with examples of how a Licensee may satisfy the requirements laid out in the Cyber Security Rules.

Background

In October 2020 we published a detailed overview of the draft cyber security rules, which at that time were subject to industry consultation. Feedback to the consultation was received from all industry sectors (see Commission feedback report and the 'overwhelming majority' of respondents were reported to be in favour of the proposals.

Following the conclusion in November 2020 of the consultation process, the Commission issued the final form Cyber Security Rules, with Guidance, on 5 February 2021, as published on its website on 15 February 2021. The Cyber Security Rules came into force on 8 February 2021 and Licensees have **until 9 August 2021** to implement changes to their internal controls to ensure compliance.

According to research by the Ponemon Institute commissioned by security firm Keeper Security *'70% of UK financial firms suffered a cyberattack in 2020'* and *'over half (57%) of companies in the UK finance sector believe cyberattacks are increasing in severity as a result of their staff operating in remote environments'*. The same research highlighted that *'half (50%) of UK finance companies say they still don't have adequate cyber-incident response plans in place'*.

In such a landscape, the Cyber Security Rules are a welcome addition to Guernsey's forward thinking and stable regulatory regime.

Cyber Security Rules – An Overview

The Cyber Security Rules remain materially unchanged as against the consultation draft. The detail of the Cyber Security Rules are as follows:

Identify

Licensees must ensure that they have taken steps to identify the assets (including data) they hold and to assess the damage to their business if they were to lose access to those assets or if those assets were otherwise the subject of a cyber-security breach. 'Assets' are not limited to traditional IT assets and should include systems, people and data assets.

The Commission expects the Board to evaluate the cyber risks associated with the assets that the Board has identified and review the impact that a cyber-security event would have on the integrity, availability and confidentiality of those assets.

Protect and Detect

Licensees must ensure that they have appropriate policies and controls in place to mitigate any identified risks and to ensure the delivery of critical infrastructure during and following a cyber-security event.

The Guidance categorises 'controls' under the following headings:

Technical Controls - which result in security measures executed or controlled through computer systems, such as network monitoring tools, patch management, two/multi-factor authentication, antimalware software, email protection tools (phishing) and mobile device management.

People Controls - which enable staff to do their job as well as keep the business secure, such as staff training, phishing testing and the systematic delivery of awareness programs.

Administrative Policy and Governance Controls – which define a Licensee's position on security. Licensees are required to, among other things:

- create and maintain their security policies and procedures to help protect their data and other assets
- when creating a security policy, bear in mind the core objectives of confidentiality, integrity and availability of assets
- conduct regular reviews of their security tools, products and services to ensure, amongst other things, that they remain fit for purpose and provide appropriate protection for the risks the Licensee faces
- ensure that reporting to the Board on cyber matters is fit for purpose and that meaningful data is supplied to the Board concerning:
    - current cyber-security risks
    - emerging risks, threats and vulnerabilities
    - incidents, and
    - compliance status.

Licensees must also ensure that they have appropriate mechanisms in place in order to identify the occurrence of a cyber-security event.

Respond and Recover

Licensees must be able to demonstrate that they have a plan in place which aims to mitigate any disruption caused by a cyber-security event (including knowledge of and the ability to demonstrate the appropriateness of any group plan that the Licensee may form part of). Such strategy should include recovery planning and ensuring that the Licensee has adequate online and offline data backups. Where the maintenance or recovery of a Licensee's cyber-security systems is outsourced to a third party, the Licensee must be able to demonstrate that it is aware of any plan that has been put in place by that provider and that the plan is appropriate to the Licensee. Licensees must also be able to demonstrate that they are aware of the steps to be taken to restore business capabilities following a cyber-security event (eg through the maintenance of a documented and rehearsed incident response plan) and that essential activities are capable of being undertaken in the interim period.

Notification Requirements

Licensees must notify the Commission upon becoming aware of a cyber-security event which has resulted in:

- any loss of significant user data
- significant loss of availability to IT systems
- significant cost to the business
- significant loss of business capability, or
- significant loss of service to users.

The notification must include the following details pertaining to the cyber-security event:

- the date on which it was discovered
- the date on which it occurred
- its nature

- current resulting consequences
- any possible future consequences
- actions taken to mitigate the consequences, and
- any further steps to be taken.

Implementation and penalties for non-compliance

As the Cyber Security Rules have direct application to all Licensees, the penalties for non-compliance are those set out in the relevant Guernsey regulatory laws to which a particular Licensee is subject.

Impact on Guernsey Licensees

Compliance

The Cyber Security Rules require that a Licensee has appropriate policies, procedures and controls in place to mitigate the risk posed by cyber-security events. Any policies, procedures and controls adopted by a Licensee must reflect the Cyber Security Rules and take into consideration the Guidance. The Board, or equivalent, is ultimately responsible for ensuring that the Cyber Security Rules are followed.

Respond and Recover

The Commission expects all Licensees to be able to evidence that they have considered possible disruption scenarios relevant to their business which may be caused by a cyber-security event.

Judgement

The Commission recognises the requirement to use judgement when considering various matters within the rules. For example:

- the requirements in the Cyber Security Rules are often expressed to be complied with in accordance with the 'size, nature and complexity' of a Licensee's business
- the Commission may in its absolute discretion exclude or modify the application of any provision of the Cyber Security Rules to a particular Licensee, and
- the Commission recognises certain materiality thresholds, for example the Guidance notes that an internal antimalware system blocking a virus should not automatically be considered a 'cyber-security event' (which would amongst other things trigger a Commission notification requirement).

Record keeping

When seeking to implement appropriate controls, documenting the same is key. All Licensees must be able to provide evidence to the Commission on request that the Cyber Security Rules have been considered and implemented. The Commission notes that 'both incident response and recovery plans could be considered as standalone documents or could be included as part of a Licensee's business continuity and disaster recovery plans'.

Ongoing review

All relevant measures adopted by a Licensee in order to comply with the Cyber Security Rules must be reviewed both periodically (with intervals not exceeding 24 months) and in response to any trigger or cyber-security events and such reviews must be recorded by the Licensee.

Notification

The notification requirements under the Cyber Security Rules are in addition to, and not intended to replace, any separate notification obligations a Licensee may otherwise have.

Updates to Guidance following consultation

Following the consultation, the Commission has made certain additions to the Guidance, the most interesting are below:

Accreditation

The Commission notes that accreditations from a recognised body, such as Cyber Essentials, Cyber Essentials Plus or ISO270001 may help a Licensee in meeting some of the requirements set out in the Cyber Security Rules, but accreditation alone will likely not be sufficient to ensure full compliance.

Outsourcing

The Guidance reiterates that the Board must maintain oversight of any outsourced operations and that the Board retains ultimate responsibility for compliance with the Cyber Security Rules. This includes assets stored in cloud storage (or similar), which should be clearly identified.

Review

In addition to the other reporting and review requirements set out in the Cyber Security Rules, the Board should report to their shareholders on an annual basis that they are comfortable with their cyber policies, controls and reporting.

Encryption

Licensees should consider encrypting their data, including on removable storage and mobile devices or when data is sent across an untrusted network.

Policies

Licensees should consider an Access Management Policy, in addition to the other areas identified in the Cyber Security Rules, as part of their minimum expected policy and procedure considerations.

Contacts

Helen Wyatt
Partner I Advocate
Mourant Ozannes (Guernsey) LLP
+44 1481 731 408
helen.wyatt@mourant.com

Alasdair McKenzie
Associate I Solicitor (England & Wales) non-practising
Mourant Ozannes (Guernsey) LLP
+44 1481 731 506
alasdair.mckenzie@mourant.com

2021934/8 10 06 69 2/1