UPDATE

OCTOBER 2020

mourant

GFSC Consultation on Cyber Security Rules and Guidance: An Issue for the Boardroom

Update prepared by Helen Wyatt (Partner, Guernsey) and Alasdair McKenzie (Associate, Guernsey)

The Guernsey Financial Services Commission (**GFSC**) has issued a consultation paper seeking feedback on its proposal to introduce Cyber Security Rules (the **Cyber Security Rules**). The proposal follows on from the GFSC's 2019 Cyber Risk Thematic, which suggested that local industry supported a set of rules and guidance that follows five core principles, namely Identify, Protect, Detect, Respond and Recover. The draft Cyber Security Rules are now subject to consultation until 2 November 2020 after which the GFSC intends to issue a final set of rules and guidance with direct application to all licensees licensed under Guernsey's regulatory laws (**Licensees**).

Background

The Cyber Security Rules represent an international trend towards regulators placing increased importance on the risks surrounding cyber-security. Historically, the GFSC has always recognised that cyber and information security is a high priority risk area for organisations of all sizes and has issued several cyber-security related guidance notes (see here in 2016 and here in 2018.

The increase in home-working as a result of the Covid-19 pandemic, together with recent high-profile cyber-crime sanctions (see here) highlight the importance of Guernsey's regulator implementing a cyber-security regime which both mandates and guides licensees towards compliance in this complex and rapidly evolving area of risk.

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 GFSC will expect the board of directors of all Licensees (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 GFSC 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 defines 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 GFSC 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

It is proposed that the Cyber Security Rules would be imposed as a set of mandatory rules through the power afforded to the GFSC to implement such rules under Guernsey's regulatory laws. As the Cyber

Security Rules will have direct application to all Licensees, the penalties for non-compliance will follow 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 any guidance issued by the GFSC. The Board, or equivalent, is ultimately responsible for ensuring that the Cyber Security Rules are followed.

Judgement

In seeking to implement the proposed Cyber Security Rules, the GFSC 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 GFSC may in its absolute discretion exclude or modify the application of any provision of the Cyber Security Rules to a particular Licensee, and
- the GFSC will recognise certain materiality thresholds, for example the GFSC 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 GFSC notification requirement).

Record keeping

When seeking to implement appropriate controls, documenting the same will be key. All Licensees must be able to provide evidence to the GFSC on request that the Cyber Security Rules have been considered and implemented. The GFSC 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.

Home working

On 7 July 2020, the GFSC published a (non-exhaustive) list of risks and relevant considerations relating to home working. In conjunction with the consultation on the proposed Cyber Security Rules, the GFSC also welcomes feedback on this self-assurance paper. The paper will be useful to Licensees as part of the consideration of their wider cyber-security risk exposure.

Conclusions

The proposed Cyber Security Rules make it clear that cyber-security is not just an 'IT issue' but rather that cyber-security should form an integral part of any organisation's risk management approach, with responsibility for compliance sitting at Board level.

By seeking to provide a visible framework of mandatory compliance, together with useful guidance to assist Licensees, the proposed Cyber Security Rules are a welcome addition to Guernsey's forward thinking and stable regulatory regime.

The Cyber Security Rules provide both certainty of obligation together with the flexibility to tailor requirements to the nature of a particular Licensee's business and allow for the exercise of practical

judgement when considering, for example, the materiality threshold for triggering a notification requirement.

Local Guernsey businesses seeking to respond to the consultation have until 2 November 2020 to do so via the following link here.

Contacts

Helen Wyatt
Partner, Mourant Ozannes
Guernsey
+44 1481 731 408
helen.wyatt@mourant.com

Alasdair McKenzie
Associate
Guernsey
+44 1481 731 506
alasdair.mckenzie@mourant.com