Guernsey Financial Services Commission

Feedback on the Commission's Consultation Paper on Cyber Security Rules and Guidance

Issued 15 February 2021

Contents

Background

On the 21st September 2020 the Commission published a consultation paper on its proposed Cyber Security Rules and Guidance. The Consultation period ran for 6 weeks until 2nd November 2020.

There was a healthy response to the Consultation Paper which saw 39 response, mainly via the Commission's Consultation Hub.

Details regarding the principles based rules and accompanying guidance can be found on the Consultation Hub.

Cyber Security Rules and Guidance Consultation Paper - Guernsey Financial Services Commission - Citizen Space (gfsc.gg)

General overall feedback and comments

Who Responded?

Feedback and comments were received from all industry sectors, either from Firms themselves or via their industry body. The Commission also received feedback from third party consultancies and service providers as well as other official bodies.

What was the general message in the feedback?

The message from the overwhelming majority of respondents was positive and supportive of the Commission's decision to publish rules and guidance.

Support for the Commission's approach of a set of principles based rules, based on the NIST framework was also widely supported by the vast majority.

Two respondents suggested that rules were not required and guidance alone should be sufficient, or a "carve out" should be available to Firms who were managed by other Licenced Firms.

Throughout the feedback a number non-regulated non-financial services businesses (generally consultants) commented that the rules should be more prescriptive and requested that some portions of the guidance should be moved into the rules. Similarly these respondents also suggested more rigorous and strict controls should be put in place that the Commission has proposed in the rules and guidance.

Various parties suggested that the Rules could mandate that firms obtain a third party certification in relation to their cyber security, with Cyber Essentials and ISO27001 both mentioned. Likewise there were some proposals that each firm should be required to appoint a CISO (Chief information security officer) and or a named board member who was specifically responsible for Cyber Risk.

Overall, Licenced Firms were the most supportive group of respondents in regard of the Rules and Guidance in their draft form, although there were requests from some respondents for further clarity, guidance or definitions in relation to some terms used.

What are the Commission going to do next?

The Commission intends to publish its Cyber Security Rules and Guidance with some minor amendments following the consideration of the valuable feedback provided. Although the Rules come into force with immediate effect, a transition period of 6 months has been put in place to allow Firms to update their internal controls and processes in order to comply with the Rules.

Please find below comments and actions taken in relation to some of the high level feedback we have received.

The Commission is not proposing replacing the Rules with Guidance only, or offering a "carve out" for "managed" Firms. The Commission has amended its Guidance note to reference how

Boards of Firms that place heavy reliance on outsourcing partners should consider those outsourced function when ensuring that they apply the Rules and Guidance appropriately.

During the 2019 thematic feedback presentations to industry the Commission outlined its intention to produce high level principles based Rules with more specific practical Guidance. The Commission is still of the opinion that this is the most appropriate course of action and does not intend to make the Rules more specific or onerous. This approach allows for a proportionate implementation of the Rules given the wide variety of Firms subject to them.

The Commission does not consider it appropriate for all Firms to be required to appoint a CISO or nominate a named Board member to a position of Cyber accountability. Firms of different sizes and complexity will have different requirements in relation to their Cyber risk and should make appointments appropriately. Similarly, firms may wish to consider accreditation to an international standard, such as those promoted by the National Cyber Security Centre, part of the Foreign and Commonwealth Office, if it is appropriate for their business. Accreditation alone however is unlikely to result in compliance with these rules. This is in line with the risk based approach outlined in the guidance paper.

The Commission has deliberately left some terms undefined in order that Firms are able to interpret them in the direct context of their own circumstances. In response to the feedback mentioned above some additional examples have been provided in the guidance.

Specific Feedback

The below specific feedback has been collated on a principle by principle basis considering both the Rule and the accompanying Guidance. The Commission has reacted to the below feedback by making some changes to the Rules and Guidance where appropriate, as set out below.

Application and Operation

Responses from the consultancy sector state that 24 months is too long a time frame for periodic review and should be replaced by annually.

The Commission recognises that 24 months is a significant length of time in the context of cyber and encourages Firms to conduct periodic views on a frequency appropriate for their business.

Identify

A number of Firms requested that the terms "Material Asset" and "Significant" be defined.

The Commission accepts that these definitions are not clearly articulated, however this allows Firms to interpret them specifically in the context of their own circumstances. The Commission is not proposing to define these terms any further.

Three firms commented on the use of cloud services and the effect that this has on the identification of assets.

The Commission has updated its guidance to reference expectations relating to cloud services, similar to any other outsourced service.

Respondents identified and inconsistency of terms within Rule 2.1.

For the sake of consistency the title of the rule has been updated to;

Risk Assessment of Cyber Vulnerabilities and Risks

Protect

A significant comment was raised in regard to the requirement to "ensure the delivery of critical infrastructure during and following a cyber security event." It was suggested that the current wording could result in a breach of the rules on any occasion where a cyber security event resulted in the unavailability of said infrastructure or service.

The wording in 3.1 (1) of the Rules has been amended to;

"to ensure, where possible, the delivery of critical infrastructure during and following a cyber security event."

Detect

Some respondents questioned if the Rule requiring the identification of a cyber security event was achievable, or if there was a time frame required for detection.

The Commission recognises the concern raised and has updated the guidance to reflect the understanding that some events may be difficult to detect or may be detected after a long dwell time. The Detect Rule has been put in place to require Firms to have a suitable detection framework in place but the Commission understands that 100% detection is sometimes unachievable and the guidance notes this.

Various additional controls were also proposed by a number of respondents including, Encryption of data and Access Management policy.

Guidance updates have been made.

Respond and Recover

Some minor amendments to the language used in the Guidance was suggested to clarify the requirement under *5.1 (1) The licensee must be able to demonstrate that it has a plan in place which aims to mitigate **any** disruption caused by a cyber security event.*

The Commission recognises that the not all disruption can be mitigated and although the aim should remain to mitigate any disruption this will not always be possible. Some updates have been made to the Guidance in this regard.

A number of respondents raised comments regarding the guidance on Backups. Comments included the challenge that suggesting Backups "offline" was not feasible in all cases and may have the unintended consequence of forcing Firms to use outdated technology. The frequency of Backups was also challenged and it was suggested that the guidance for data to be backed up in "real time" may not always be appropriate.

Guidance has been amended to consider the feedback provided.

"A Firm should ensure it has adequate backups both online and where appropriate, offline or unconnected to a Firm's main network. Online backups should be connected to systems, and be backed up in real time or at a frequency agreed in the Firms relevant policies and procedures, and offline, or unconnected, backups should not be connected to the network so that they cannot be themselves corrupted in the event of ransomware."

Notifications and General Provisions

The notification requirements were well received and Firms stated that the examples provided in the Guidance provided useful assistance. One recipient was concerned that the notification requirements introduced a dual reporting regime to both the Office of the Data Protection Authority and the Commission, while others recognised the value of reporting to both organisations.

Reporting to the Commission is a separate requirement to that under the Data Protection (Bailiwick of Guernsey) Law 2017 and although a Firm may be required to report similar incidents it is essential that notification is made independently. The Data Protection Commissioner's considers cyber risk events within the wider context of its role as the independent authority responsible for regulating the Bailiwick's data protection law. The ODPA's focus is on ensuring all entities who use people's data meet their legal obligations, respect people's rights, and consider ethical data use, while the Commission considers the effect of a cyber-event on the wellbeing of the firm and the customers it serves.

There were some comments requesting clarity on the definition of "significant", which is used throughout the notification requirements in the rules and requesting that the Commission give an indication of the required timeframe for notifications.

As discussed previously in this paper, the use of the term "significant" allows for each Firm to apply the rules appropriately for the size and complexity of its business.

The Commission has updated the guidance to provide some indication that notification to the Commission should be made as soon as is practical but will depend on the specific incident in question. The Commission recognises that a notification may come in multiple tranches as information relating to the incident, its impact and the firm's actions become available.

The Commission's self-assurance paper on home working

There were no significant comments made on this paper, which was well received.