ISLE OF MAN
FINANCIAL SERVICES AUTHORITY

Lught-Reill Shirveishyn Argidoil Ellan Vannin

REGULATORY GUIDANCE

Cyber Security

December 2016

(last updated Jun 2023)

V.01 issued 12 December 2016
V.02 issued 23 September 2020
V.03 issued 27 June 2023

Glossary

Term	Meaning in this document
Authority	Isle of Man Financial Services Authority
CGC2010	Corporate Governance Code of Practice for Regulated Insurance Entities (applicable to insurance managers)
CGC2020	Insurance Intermediaries (Corporate Governance)(General Business) Code 2020 (applicable to insurance intermediaries)
CGC2021	Corporate Governance Code of Practice for Insurers 2021 (applicable to authorised insurers and permit holders)
CISA2008	Collective Investment Schemes Act 2008
FSA2008	Financial Services Act 2008
IA2008	Insurance Act 2008
RBSA2000	Retirement Benefits Schemes Act 2000
Rule Book	Financial Services Rule Book 2016

1. Cyber security

1.1. Introduction

The frequency, sophistication and cost of cyber attacks are continually increasing. Additionally, financial service providers are particularly exposed to the risks associated with cyber attacks because they often receive, hold and transfer large sums of money. Likewise they tend to collect and store substantial amounts of private and confidential client information, and that information may also be shared with various third parties (e.g. outsourced service providers).

Successful cyber attacks can result in the loss of assets or confidential information or cause considerable disruption to business services, which may subsequently cause significant damage to the reputation and financial performance of affected businesses, as well as significant and long-term detriment to affected clients. Successful cyber attacks also have the potential to undermine confidence in the Island's financial services sector as a whole.

Consequently, the Authority wishes to highlight the risks of inadequate cyber security to regulated entities and draw attention to a number of key legal and regulatory provisions that are relevant to this issue.

This guidance aims to help regulated entities understand the Authority's expectations and to comply with existing requirements. This guidance does not modify any existing requirements or impose any additional obligations on regulated entities. The practices and suggestions in this guidance may not be relevant or appropriate in every case, and the guidance is not intended to be exhaustive. The Authority issues guidance for various purposes, including to illustrate best practice, to assist relevant persons in complying with legislation and to provide examples or illustration. This guidance has been issued under section 12 of the FSA2008, section 34 of the IA2008 and section 42 of the RBSA2000. This guidance is not law, however it is persuasive. Where a person follows guidance this would tend to indicate compliance with associated legislative provisions, and vice versa. **For the avoidance of doubt, this guidance does not constitute binding guidance under the IA2008.** Original legislation should always be consulted for legal purposes. If you are unsure about your legal obligations you should seek legal advice.

1.2. Types of attacks and practical measures

Types of cyber attacks include hacking, phishing, malware and denial of service attacks.

- Hacking involves someone gaining unauthorised access to a computer or network, usually by exploiting an existing weakness in security settings or using stolen credentials. Hacking techniques include password cracking, Trojan horses and key loggers.

- Phishing usually involves fake emails or instant messages that appear to come from legitimate businesses. The emails and messages typically contain URLs that link to malicious web pages which may look almost identical to legitimate sites. Clicking on the link may allow malware to be installed or the fake website may trick the end user into entering confidential information such as passwords or bank account details (often the emails and messages encourage the end user to update, validate or confirm an account and they may appear to be official, use threatening language or create a sense of urgency). The information acquired by the criminals is then used to commit identity theft, gain access to bank accounts, etc. Phishing emails often contain a number of subtle warning signs, for example one letter in the sender's email address may be different to the genuine email address, the greeting may not be personalised, the email may contain grammatical errors and spelling mistakes, or the email may create a sense of urgency. However, cybercrime is becoming increasingly sophisticated and consequently it is becoming more difficult to differentiate between legitimate and bogus emails. The global Covid-19 pandemic has caused a surge in phishing and ransomware attacks across various industries worldwide. The increased frequency and severity of cyber-attacks coincides with increased home working, digitalisation and use of third-party services such as cloud services.

- Malicious software, commonly known as malware, is any software that adversely affects a computer or computer system. There are several types of malware, including computer viruses, worms, adware and spyware. There are also advanced types of malware, for example ransomware which is used to extort money. Ransomware incidents are increasingly common and they typically involve files on a computer being encrypted to prevent access to them (encryption ransomware) or completely preventing access to a computer (lockscreen ransomware). Money will then be demanded to regain access to the computer or to decrypt or not publish the compromised data. Certain types of ransomware are very effective, and victims of such attacks may be unable to retrieve data (even if they pay the ransom) unless they have made a backup copy. A Trojan horse (or Trojan) is commonly used to trick end users into installing malware – this is typically achieved by hiding malicious software within a seemingly innocent looking email attachment such as an invoice or picture, a link to a bogus website which may appear to be legitimate (often the link will direct the user to a web page that is different to the URL displayed in the email) or a free program such as a game. The malicious software is downloaded when the recipient opens the attachment, clicks on the link or downloads the free program. Alternatively, scareware may be used to intimidate the end user into taking action – a common form involves a pop up message which states that the computer has a security problem. Once activated, the malicious software can enable cyber criminals to spy on the user, steal confidential data such as bank account details and passwords, and give them remote access to the computer. Emails containing malware may often be received from an unknown sender, however bogus emails can also appear to come from someone known to the recipient, for example, where a cyber-criminal has created an email address that is almost identical to a genuine email address or a virus has been

used to spoof the return address. Consequently, malware is often unwittingly downloaded from an email attachment or from a bogus website.

- Denial of service attacks allow attackers to bring down a network without having to gain internal access; this is achieved by flooding the access routers with fake traffic and overloading the system until it fails. There are also distributed denial of service attacks, which are coordinated denial of service attacks from multiple sources. The ultimate aim of a denial of service attack may simply be to cause disruption by bringing down the network, alternatively they may be used as a mechanism to extort money or to create a distraction to facilitate another attack.

Every person and business is vulnerable to cyber attacks. However, there are a number of practices that can significantly increase your protection from the majority of attacks. These include taking simple steps such as choosing strong passwords that contain a mixture of capital and lower case letters, numbers and symbols and changing passwords frequently, keeping operating systems, software and web browsers up to date and installing anti-virus software and firewalls. Network and system access could also be restricted to users using the principle of least privilege, whereby users and other applications/systems are given the minimum levels of access or permissions needed to perform their job or task. Most advanced cyber attacks rely on exploiting privileged credentials; therefore limiting such privileges helps reduce both the risk and impact of a cyber attack. It is very important to ensure that there are adequate processes in place to regularly monitor and re-grant/revoke permissions to ensure that all users continue to have only the minimum levels of access required.

1.3. Legal and regulatory requirements

Appendix 1 consists of a table which summarises some of the key legal and regulatory provisions that are relevant to cyber security in the Rule Book made under the FSA2008 and the CGC2010, CGC2020 and CGC2021 issued under the IA2008. Designated insurers are also subject to provisions which are relevant to cyber security in the Insurance (Group Supervision) Regulations 2019 (including regulation 5(1) (fitness and propriety); regulation 7 (policies and procedures); regulation 8 (corporate governance); and regulation 9(1) (reporting)), and those Regulations are supplemented by further provisions in relation to corporate governance frameworks, including enterprise risk management systems, in the Corporate Governance Code of Practice for Designated Insurers.

The table also includes comments regarding the Authority's expectations in relation to those provisions and some examples of best practices to help regulated entities to determine whether their cyber security framework is effective, and to provide for a systematic and proactive approach to managing existing and emerging cyber threats. However, it is regulated entities responsibility to determine what their legal obligations are and to evaluate their exposure to cyber risk and decide how best to manage it.

In addition, the FSA2008, the IA2008, the RBSA2000 and the CISA2008 all contain provisions regarding the fitness and propriety of certain persons and entities regulated under those Acts.

Consequently, when assessing fitness and propriety (as part of an application process or on an ongoing basis), in appropriate cases, the Authority may consider issues relevant to cyber risk. For example, the Authority may consider whether an applicant, especially one whose business model is highly IT dependent, has an effective cyber security framework in place which provides a systematic and proactive approach to managing existing and emerging cyber threats.

Section 41 of the RBSA2000 also provides that specified persons, including the trustee and administrator of any retirement benefits scheme, must notify the Authority if they have reasonable cause to believe that any duty relevant to the administration of the scheme is being, or has been, breached, where the failure is likely to be of material significance in the exercise by the Authority of any of its functions. Therefore, relevant regulated entities and persons should promptly notify the Authority of any serious or significant incident involving data loss, financial loss, disruption to services or denial of services type attacks.

The Data Protection Act 2018, together with the Data Protection (Application of GDPR) Order 2018, the Data Protection (Application of the LED) Order 2018 and the GDPR and LED Implementing Regulations 2018 made under that Act, also impose certain requirements in relation to the way personal data is used by businesses. In particular, businesses using personal data must follow the principles relating to the processing of personal data set out in article 5 of the Applied GDPR in the Annex to the Data Protection (Application of GDPR) Order 2018, which include a requirement to take appropriate technical or organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Further information in relation to data protection law is also available on the Isle of Man Information Commissioner website.

The table in Appendix 1 primarily sets out requirements in/under the FSA2008 that are applicable to licenceholders and requirements in/under the IA2008 that are applicable to insurers, insurance intermediaries and insurance managers. However, administrators and trustees of retirement benefits schemes regulated under the RBSA2000 must remain fit and proper and comply with the Data Protection Act 2002, therefore it is recommended that trustees and administrators who control or process members' personal data and/or hold or control scheme assets also refer to the commentary in the table in Appendix 1 for guidance in relation to cyber security matters.

1.4. Examples of incidents

A number of anonymised examples of actual cyber security incidents that have occurred locally have been set out in Appendix 2.

1.5. Other resources

Finally, links to a number of white papers and websites have been provided in Appendix 3. These resources do not constitute regulatory guidance; however, they may provide regulated entities with useful information and practical guidance.

The Authority is not responsible for the availability or content of these resources.

Appendix 1 – Key legal and regulatory requirements under the FSA2008 and IA2008

This Appendix contains a summary of, and commentary in relation to, key rules in the Financial Services Rule Book 2016 ('Rule Book') made under the FSA2008 in the context of cyber security.

This Appendix also contains a summary of, and commentary in relation to, key provisions in the CGC2010, CGC2020 and CGC2021issued under the IA2008 in the context of cyber security.

1	Cyber Security Framework & Governance			
	Rule Book	CGC	Summary	Comments
Rule 8.2		CGC2010: Para 3.3 CGC2020: Para 7 CGC2021: Para 7	The Rule Book, sections 17A and 27D of the IA2008 and the CGC2010, the CGC2020 and the CGC2021 contain provisions that broadly require regulated entities to have in place appropriate arrangements for effective corporate governance.	• Sound governance is key to the effective management of all forms of risk, including cyber risks. • In particular, the engagement and commitment of the board and senior management is essential, as this will help to create organisation-wide support for cyber risk management and enable appropriate resources and expertise to be made available to address cyber risks. • Examples of best practices include – ○ promotion of organisation-wide support for cyber risk management by the board; ○ regular inclusion of cyber security on board agendas; ○ appointment of someone suitably senior within the organisation to be responsible for cyber security matters. This could, for example, be a senior manager with appropriate knowledge and

				experience or a board member who has received appropriate training; ○ establishing the risk tolerance of the firm and overseeing the design, implementation and effectiveness of a cyber security framework which is tailored to the nature, size, complexity, risk profile and culture of the business; ○ articulating lines of reporting and escalation.
2	**Risk, Controls and Monitoring**			
	Rule Book	CGC	Summary	Comments
2.1	Rules 8.3 and 8.6	CGC2010: Paras 7.12, 7.13, 9, 15, 16 and 17 CGC2020: Paras 24 and 26 CGC2021: Paras 9, 36, 37, 42 and Part 11 and Part 12	The Rule Book, the CGC2010, the CGC2020 and the CGC2021 contain provisions that broadly require applicable regulated entities to establish and maintain an effective risk management framework for managing the risks associated with their business, including all operational risks, as well as a requirement to establish and maintain appropriate internal controls relating to all aspects of their business. These provisions also require applicable regulated entities to monitor the relevant risks on an ongoing basis.	• Where relevant legal and regulatory requirements apply, the Authority expects regulated entities to – ○ identify and assess risks associated with IT vulnerabilities such as cyber attacks as part of their risk management framework; ○ implement appropriate and effective controls, for example systems, policies, procedures and training initiatives, to help protect against and manage the risks associated with cyber attacks; ○ proactively monitor activity within your network to detect potential cyber incidents; ○ review, and where appropriate revise, the controls associated with cyber threats at appropriate intervals. • Former and current employees, contractors, consultants and third party service providers can be a significant source of cyber incidents (which may be
2.2	Rules 3.37(6), 8.3(2)(h) and 8.6(4)(a)(iii)	CGC2010: Paras 5.7 and 7.11(c)	There are also a number of specific provisions in the Rule Book, the CGC2010, the CGC2020	

		CGC2020: Paras 24(2)(d), (e) and (f) CGC2021: Paras 13, 14, 35(c) and 73(2)(f)	and the CGC2021 in relation to safeguarding data and assets.	deliberate or unwittingly facilitated), therefore this should be taken into account within the risk management framework and associated internal controls. • Cyber criminals also often target consumers directly, for example by using 'phishing' emails and emulating unsecured Wi-Fi facilities in public places. Therefore, the cyber risks associated with such practices should also be taken into account. • Examples of best practices include – ○ identification of functions, activities, systems, assets, information, products and services – including interconnections, dependencies and third parties – prioritising their relative importance, and assessing their respective cyber risks; ○ implementation of appropriate policies and procedures, including procedures to verify the legitimacy of all requests received by all methods of communication (the verification procedures should require the verification of *all* details, for example, including the beneficiary's name and bank details rather than just the amount in relation to payment requests); ○ management and control of user privileges, control of removable media usage, and monitoring of mobile and home working procedures;
2.3	Rule 8.3(4)(a)	CGC2010: Paras 5.6, 7.1(d), 9(a) to (c), 12.3(b) and (c), 13.4, 16.2(b), and 17(c) CGC2020: Paras 9 and 24(4) and (5) CGC2021: Paras 12, 26(4), 42(a) to (c), 50(2)(b) and (c), 55,	The Rule Book contains provisions which require regulated entities to ensure staff and others who conduct regulated activities that they are responsible for are suitable, adequately trained, properly supervised and do not exceed any limitations placed on those persons. Similarly, the CGC2010, the CGC2020 and the CGC2021 require regulated entities to have an appropriate level of management, with adequate and competent staffing and resources, that provides for its sound and prudent management. There are also provisions in the CGC2010 and the CGC2021 which broadly require regulated entities to establish, implement and maintain internal strategies, policies and procedures in order to ensure that the regulated entity complies with its legal and regulatory	

		68(1)(b), 69(c) and 73(1)	obligations, including provisions which require various levels of oversight, checks and balances, and, where appropriate, training for staff.	○ ensuring that systems are secure, for example, by keeping operating systems, software and web browsers up to date, installing anti-virus solutions on all systems, backing up important information on a regular basis (it is advisable to store backup files in a secure offsite location), and ensuring that mobile devices with access to their systems are secure (e.g. via encryption and password protection using strong passwords); ○ monitoring the use of all equipment and IT systems to detect anomalies and events indicating a potential cyber incident; ○ ongoing cyber awareness and training initiatives to ensure that staff understand the risks associated with cyber attacks and the procedures that have been put in place to mitigate the risks associated with the same; ○ if a firm is involved in payment card processing or it stores, processes or transmits cardholder data and/or sensitive authentication data, it should consider the best practices set out in the Payment Card Industry (PCI) Data Security Standard; ○ conducting cyber security tests, for example penetration testing of systems (firms may wish to consider engaging the services of an external specialist to carry out such tests); ○ keeping up to date on current cyber threats and where appropriate revising controls accordingly – being alert and responsive to new cyber threats is

				crucial given the escalating risks that cyber threats pose.
3	Outsourcing			
	Rule Book	CGC	Summary	Comments
3.1	Rule 8.16	CGC2010: Paras 7.1, 7.5 and 10 CGC2020: Para 30 CGC2021: Paras 26, 30 and 43	Provisions in the Rule Book, the CGC2010, CGC2020 and the CGC2021 also contain a number of requirements in relation to outsourcing and delegation.	• Where the relevant provisions require a written agreement between the regulated entity and the service provider, that agreement should include the respective responsibilities of the parties to it. Consequently, such an agreement may need to include provisions dealing with each respective parties responsibilities relating to IT security. • Whether an activity constitutes a material management or business function/significant outsourced function will depend, for example, on the nature of the business concerned and the services that have been outsourced. However, the significance of the risks that service providers pose is not necessarily proportionate to the materiality of the service that is outsourced or delegated. Therefore, the risks in relation to all outsourced services and delegated functions should be managed as part of the broader risk management framework, for example by taking measures to prevent access to systems and confidential data or taking appropriate measures to determine that service providers have appropriate and adequate cyber security standards and procedures in place to protect assets and client related information.

				• In relation to delegations which are subject to rule 8.16(1) of the Rule Book, the Authority may, in appropriate cases, consider whether a licenceholder has taken such appropriate measures prior to granting consent.
4	**Contingency Planning & Incident Response**			
	Rule Book	CGC	Summary	Comments
4.1	Rule 8.14(1)	CGC2010: Para 5.10 CGC2020: Para 13 CGC2021: Para 16	Provisions in the Rule Book , the CGC2010, CGC 2020and the CGC2021 broadly require applicable regulated entities to establish and maintain appropriate business resumption and contingency arrangements.	• Where relevant legal and regulatory requirements apply, regulated entities ought to have in place business resumption and contingency arrangements which would enable them to suitably respond to, and recover quickly from, a successful cyber attack. • The associated policies and controls should clearly set out decision making responsibilities, define escalation procedures and establish processes for communicating with appropriate stakeholders (see also reporting incidents below). • In the event that a cyber incident occurs, the response should also involve an assessment of scope, nature and impact of the incident and steps to contain and mitigate the impact of it, including removing any ongoing threat such as malware. • The response and recovery plans should also take into account the fact that communication methods such as email may not be operational. • The resumption and contingency arrangements should be tested and reviewed at appropriate intervals in order to make contingency planning effective.

				• Recovery should include remediating vulnerabilities to prevent similar incidents occurring in future.
5	**Reporting Incidents**			
	Rule Book	CGC	Summary	Comments
5.1	Rules 8.17(1), 8.18(1), 8.20 (2)(a) and (i), and 8.30(b)	CGC2010: Paras 18, 17(a) and 20 CGC2020: Paras 29 and 31 CGC2021: Paras 69(a)(i), 71 and 75	• A number of provisions in the Rule Book, the CGC2010, the CGC2020 and the CGC2021 and the RBSA2000 require certain matters to be reported to the Authority. • For example, the Rule Book requires a licenceholder to notify the Authority, inter alia, where it has reason to believe that an employee is involved in fraud or it becomes aware that fraud has been committed by a third party and it may be material to the safety, soundness or reputation of the licenceholder, certain breakdowns of computer systems, the material loss of consumer or other data, and any material breach of the regulatory requirements. The Rule Book also requires licenceholders to promptly inform the Authority of anything relevant to the exercise of its regulatory functions. • Similarly, the CGC2010, the CGC2020 and the CGC2021 provide that a regulated entity must establish, implement and maintain adequate and appropriate	• Regardless of regulatory requirements, the Authority expects regulated entities to promptly notify the Authority of any serious or significant incident involving data loss, financial loss, disruption to services or denial of services type attacks. • Regulated entities should also notify the Authority of any serious or significant attacks (of which they are aware) that were **prevented**. • Information sharing provides numerous benefits, including helping the Authority to gain a better understanding of the cyber security landscape and, where appropriate, facilitating the sharing of anonymised cyber security information among industry participants in the Island. Ultimately, sharing information may reduce systemic risks by enabling regulated entities to quickly and effectively react to a cyber threat.

			policies and procedures in respect of reporting fraud to the appropriate authorities, and to encourage the reporting of any other improper or unlawful behaviour. In addition, the relevant Codes also require the regulated entity to maintain open, honest and timely communications with the Authority; and the CGC2021 includes a specific requirement to notify the Authority of anything which the Authority would reasonably expect to have notice of having regard to its regulatory objectives.	
6	Insurance Cover			
	Rule Book	CGC	Summary	Comments
6.1	Rule 8.57(3) Regulation 7 Insurance Intermediaries (General Business) Regulations 2020	No specific provisions in the CGC2010 or CGC2021. However, please see the summary and comments opposite, and note that regulated	Rule 8.57(3) of the Rule Book and regulation 7 of the Insurance Intermediaries (General Business) Regulations 2020 require certain licenceholders and insurance intermediaries to maintain a minimum level of professional indemnity insurance ('PII') cover.	• PII cover may sometimes include cyber liability cover, however, cyber liability cover is not a regulatory requirement. • Nonetheless, given that cyber security measures may not prevent all cyber attacks, this could be something that regulated entities may wish to consider as part of their overall risk management framework.

		entities' own insurance arrangements form part of their wider operational risk management.		
7	Stakeholder Interests			
	Rule Book	CGC	Summary	Comments
7.1	Rules 6.5(1) and 8.3(2)(c)	CGC2010: Paras 5.4, 7.7(c), 7.11(b)(iii), 7.15(c), 8(b), 9(c)(iii), 10(d)(iii) and 19 CGC2020: Paras 10, 24(1),24(2)(a) and (c) and 30(e)(iii)	• The Rule Book provides that a licenceholder must not carry on business of such a kind or in such a way as may be likely to bring the Island into disrepute or damage its standing as a financial centre. • The Rule Book also contains' provisions which require internal controls to ensure the fair treatment of clients. • Similarly, the CGC2010, the CGC2020 and the CGC2021 provide that a regulated entity must have due regard for the interests of its stakeholders and treat them fairly. In support of the foregoing, the relevant Codes include provisions which require the adoption of appropriate standards of conduct, effective communication systems and an	• Successful cyber attacks have the potential to cause significant and long term detriment to affected clients. • Successful cyber attacks also have the potential to undermine confidence in the Island's financial services sector as a whole. • Therefore, relevant regulated entities should ensure that these factors are taken into account within their governance arrangements and risk management framework in the context of cyber risks.

		CGC2021: 9(1)(b)(iv), 31(c), 35(b)(iii), 38(d), 39(a), 41(d) and (e), 42(a)(ii) and (c), 43(e)(iii), 73 and 74	internal corporate culture which promotes the fair treatment of stakeholders. There are also further provisions which relate specifically to the fair treatment of policyholders.	

Appendix 2 – Examples of cyber security incidents

Example 1 – Payment Requests	
What happened?	• *Several incidents in the Island have involved regulated entities receiving fraudulent payment requests by email after clients' email accounts had been hacked.* • *In another case, an employee of a regulated entity had their email account hacked and the hacker placed an auto forward rule on the employee's email account to enable monitoring over a period of time. When a client sent a number of genuine payment requests by email to the employee whose account had been hacked, the genuine payment requests were deleted by the hacker and substituted with fraudulent payment requests sent from an almost identical email address to that of the client and the requested payment amounts were the same as those in the original emails, but the beneficiary name and bank account details had been changed.* • *A number of payments ranging from £20,000 to over £1,000,000 were made by the affected regulated entities.*
What was the impact?	• *Many of the payments have never been recovered or were only partially recovered.*
How can these types of incidents be prevented?	• *There are various steps that firms can take that may help to prevent these types of incidents, including having procedures (such as call back procedures) in place to verify the legitimacy of requests.* • ***Ideally, the legitimacy of <u>all</u> requests should be verified.*** • *Otherwise verification procedures should establish appropriate triggers, for example transfers to unfamiliar accounts. Also, when establishing triggers (e.g. amount thresholds), regulated entities should also consider that sometimes frauds may be carried out as a series of transactions and the value of each individual transaction may be relatively low.* • *Also, all of the details should be verified (e.g. the beneficiary's name and bank details rather than just the amount, as a fraudulent payment request may replicate the amount in a genuine payment request).* • *As well as establishing and implementing appropriate verification procedures, cyber security awareness training and procedures to verify that employees are following the procedures that have been put in place to mitigate the risks associated with cyber threats can help to reduce the risk of non-compliance therewith.*

Example 2 – Information Request	
What happened?	• *A fraudster created an email address which was almost identical to the firm's own (one letter of the email address was different, but the fraudster used the similarity between some letters in certain fonts to create an email address which looked almost the same as the firm's own).* • *The fraudster then attempted to obtain confidential information from a member of staff by posing as a colleague.*
What was the impact?	• *No funds were lost, however a data protection breach occurred.*
How can this type of incident be prevented?	• *Again, this type of incident might be prevented, for example, by having appropriate procedures in place to verify the legitimacy of requests.*

Example 3 – Ransom Demand	
What happened?	• *A regulated entity received a ransom note from an organised cyber-crime group who attempted to extort money from the firm by threating to subject it to a substantial and sustained distributed denial of service attack ('DDoS') due to start imminently thereafter.* • *On the same day that the ransom note was received, the firm escalated the matter to its IT Security & Risk Team. The firm also immediately notified its cyber insurers who were able to provide support. In addition, the firm carried out a review to assess its technical defences and service impacts, scope of impact, legal implications and regulatory and law enforcement notifications.* • *The firm already had DDoS protection through a third party service provider; however, as a consequence of the ransom note, it brought forward a planned changeover to DDoS protection with another service provider in order to provide greater resilience to future attacks.* • *The firm ensured that a response team was available over the weekend when the attack was expected.* • *The firm's crisis team also held regular meetings to monitor the situation and ensure appropriate actions were in place to mitigate the risk. The firm also considered the possibility that the DDoS threat was being used as a distraction technique.* • *Thereafter, the firm reported the incident to the Authority and Action Fraud and continued to closely monitor the situation.*
What was the impact?	• *None (there was no data breach or interruption to services).*

How can this type of incident be prevented or mitigated?	• *There are various steps that firms can take that may help to prevent these types of incidents from occurring or help to mitigate their impact if they do occur, including having adequate and effective business resumption and contingency arrangements in place which would enable them to suitably respond to, and recover quickly from, a successful cyber attack.* • *In the event that a cyber incident occurs, the response should include taking appropriate steps to contain and mitigate the impact of it, including removing any ongoing threat such as malware.* • *See section 4 of the table in Appendix 1 for further details regarding contingency planning and incident response*.

Appendix 3 – Other resources

European Central Bank (2016) *G7 fundamental elements for cyber security* –
https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf

Gov.uk: *Cyber security guidance for business* –
https://www.gov.uk/government/collections/cyber-security-guidance-for-business

International Association of Insurance Supervisors: *Issues Paper on Cyber Risk to the Insurance Sector* –
http://www.iaisweb.org/page/supervisory-material/issues-papers/file/61857/issues-paper-on-cyber-risk-to-the-insurance-sector

International Organization of Securities Commissions (2016) *Cyber Security in Securities Markets – An International Perspective* –
https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf

International Organization of Securities Commissions (2016) *Guidance on cyber resilience for financial market infrastructures* –
https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

International Organization of Securities Commissions (2005) *Principles on Outsourcing of Financial Services for Market Intermediaries*, Topics 2 and 3 –
https://www.iosco.org/library/pubdocs/pdf/IOSCOPD187.pdf

National Association of Corporate Directors (2014) *Cyber-Risk Oversight* –
https://www.nacdonline.org/files/NACD%20Cyber-Risk%20Oversight%20Executive%20Summary.pdf

National Cyber Security Centre –
https://www.ncsc.gov.uk/

National Cyber Security Centre: *Cyber aware* –
https://www.ncsc.gov.uk/cyberaware/home

National Cyber Security Centre: *Small Business Guide: Cyber Security* –
https://www.ncsc.gov.uk/collection/small-business-guide

National Cyber Security Centre: *10 Steps to Cyber Security* –
https://www.ncsc.gov.uk/collection/10-steps

National Protection Security Authority –
https://www.npsa.gov.uk/

PCI Security Standards Council: *Document Library* –
https://www.pcisecuritystandards.org/document_library/

PwC (2016) *Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016* –
https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf