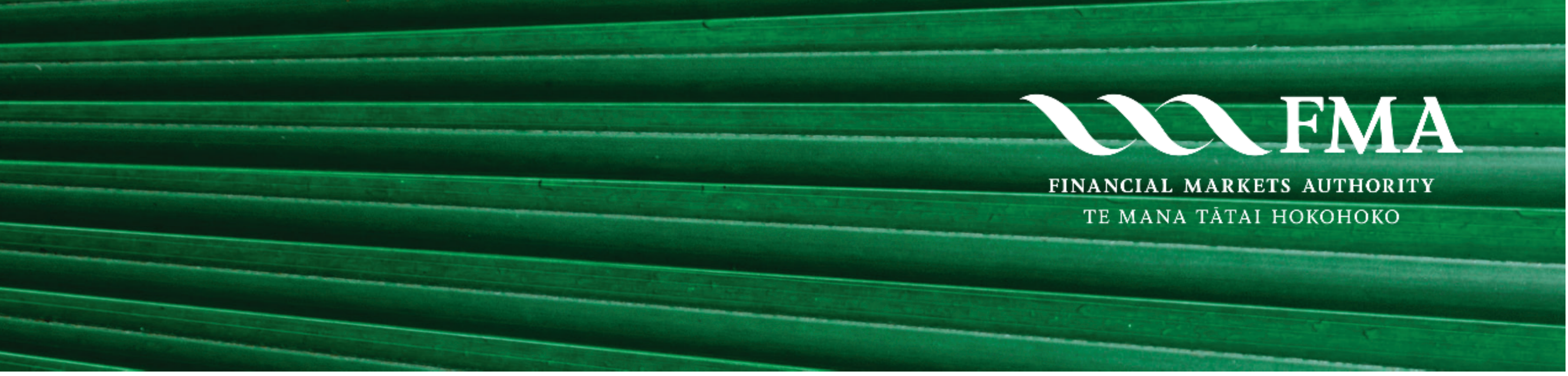

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

JULY 2021

Developing cyber resilience for financial advice providers

This information sheet assists small and medium-sized financial advice providers (FAPs) with enhancing the security and resilience of their technology systems. It does not contain an exhaustive checklist – FAPs should carefully consider the cyber threats they face and design their own policies, processes and controls to adequately address potential threats. This information may also be useful for other financial service providers.

Overview

The new financial advice regime came into force on 15 March 2021. Entities and individuals granted a full FAP licence under the Financial Markets Conduct Act 2013 (FMC Act) will be subject to the standard conditions for full FAP licences.

Standard condition 5 sets out requirements around business continuity and technology systems, particularly for maintaining information security of technology systems which, if disrupted, would materially affect the financial advice service. We consider cyber resilience fundamental to information security and continuity under Standard condition 5.

Cyber resilience

Cyber attacks on businesses in New Zealand are increasing in both sophistication and frequency. The New Zealand Computer Emergency Response Team (CERT NZ) quarterly data report consistently shows the financial services and insurance industries have the highest number of reported incidents out of all sectors in New Zealand.[1] Due to the steep increase of cyber security incidents, FAPs should adopt a proactive and preventative approach to counteract the current trend and mitigate the risks to their organisation.

FAPs also have specific obligations under the new financial advice regime to ensure that their technology systems remain secure.

Source of obligations

For a complete list of FAP obligations, visit the FMA website here.

[1] Refer to CERT NZ Quarterly reports from beginning January 2018 to ending March 2021

Standard conditions for full FAP licence	Code of Professional Conduct for Financial Advice Services (Code Standard)	FMC Act
Standard condition 5 requires FAPs to have and maintain a business continuity plan that, among other things, includes procedures for responding to, and recovering from, events that impact on cybersecurity and continuity. FAPs must ensure information security of technology systems which, if disrupted, would materially affect the continued provision of your financial advice service, is maintained. FAPs are required to notify the FMA within 10 working days of discovering any event that materially impacts the information security of these critical technology systems. Under Standard condition 6, FAPs also need to ensure that policies, processes, systems and controls are up to date and that they reflect any changes you may make to your business or service arrangements.	Code Standard 5 requires FAPs to ensure that client information is protected against loss and unauthorised access, use, modification or disclosure. This includes maintaining physical and electronic security measures so that only authorised personnel of the FAP have access to client information.	The FMC Act imposes duties on persons who give regulated financial advice and on FAPs and interposed persons that engage them. These include the duty to comply with the standard conditions of the FAP licence and the Code Standards. FAPs are also required to exercise the care, diligence and skill that a prudent person engaged in the occupation of giving regulated financial advice would exercise in the same circumstances.

Building cyber resilience capabilities

FAPs need to be aware of and take appropriate action to mitigate the cyber-related risks they face. FAPs should be prepared, and importantly, be able to resume operations without undue delay following a cyber breach. This should be done in a manner proportionate to the size and structure of the FAP's operational environment, and suited to the nature, scope, complexity and risk profile of its products and services. For example, a small business with simple processes and technology may only need a relatively brief plan covering a more limited range of likely disruptive events.

Below are some areas for small and medium-sized FAPs to consider in order to build their cyber resilience capabilities.

Arrangements for cyber risk management

This includes having adequate and effective policies, processes and controls to manage cyber risk. As part of having appropriate arrangements, FAPs should consider key attributes such as:

- regularly identifying and reviewing risks and cyber threats
- implementing measures that maintain the level of information security necessary for their risk profile
- having effective processes that monitor and detect activity that impacts information security
- including in the business continuity plan the predetermined procedures for responding to, and recovering from, events that impact information security.

FAPs should also consider conducting a cyber security risk assessment for their business. This will help FAPs understand their critical business processes, and the systems and data that need to be secured. This should include cyber risks associated with using third-party service providers. The risk assessment should be revisited regularly to ensure it captures current risks to the business.

Where multiple software applications are used, or where there is a strong reliance on staff managing security, FAPs should consider introducing strong password management controls such as using unique, long and strong passwords and two-factor authentication.

FAPs should also consider monitoring attempted cyber incidents by installing antivirus software to help detect and remove malware from computer systems. Putting in place a good back-up plan for data, for example by maintaining securely held backups offsite, will aid in recovering any information lost due to a cyber incident.

Response procedures for a cyber incident should include consideration of remediation with respect to any risks and harms experienced by customers. For example, if a customer's confidential information is stolen, we encourage FAPs to consider both the information and financial needs of customers, which may require a communication about the incident and compensation.

Regularly test systems and controls

This includes regular review and testing of cyber risk management arrangements to ensure these remain relevant for the business. This testing can be included in the FAP's compliance assurance programme.[2]

Cultivate a culture of awareness of and commitment to cyber resilience within the organisation

Boards and senior management should lead by example and provide necessary support to staff so they are aware of their responsibilities. This includes creating a culture of awareness in the organisation and building capability through continuing cyber resilience training for staff at all levels.

For example, small businesses should ensure staff (including senior management and the board) are aware of what cyber risks exist, and understand how to respond to and report them. Boards and senior management should receive sufficient reporting on cyber risk and the tools in place to monitor it.

[2] Refer to our information sheet on compliance assurance programmes for more details.

Notify the FMA of any material information security breach

FAPs should have arrangements in place to notify the FMA in the event of a material information security breach within 10 working days of the incident being identified. A material event is one where the confidentiality, integrity or availability of information and/or technology systems has been compromised. FAPs do not need to notify us of minor events, such as receiving a ‘phishing’ email.

For small business, such arrangements could mean putting together an incident response plan that sets out the course of action the organisation will take to navigate the cyber incident. One of the tasks in the plan could be identifying whether the event meets the threshold for a material event and, if it does, notifying the FMA.

FAPs should be aware of any other notification requirement mandated by legislation that may be triggered by a cyber incident. For example, under the Privacy Act 2020, if a FAP has a privacy breach that either has caused or is likely to cause anyone serious harm, the FAP will need to notify the Privacy Commissioner and any affected people as soon as practicable.

Although not mandatory, we also encourage FAPs to notify CERT NZ if they experience a cyber incident.

FMA’s cyber resilience review

In 2019 the FMA conducted a thematic review of market participants’ cyber resilience. The Cyber-resilience in FMA-regulated financial services report summarises the findings of the review and provides guidance for firms in areas where we have identified the need for improvement.

Key recommendations by the FMA for managing cyber risk include:

- *Use services provided by CERT NZ and New Zealand’s National Cyber Security Centre.*
- *Assess cyber risks as part of wider risk assessment and management programmes.*
- *Use a recognised cybersecurity framework to assist with planning, prioritising and managing cyber resilience (for example the National Institute of Standards and Technology (NIST) cybersecurity framework core).*
- *Have an appropriate balance between protection and detection measures, avoiding over-reliance on protection measures alone.*
- *Governance arrangements must include board and/or senior management ownership and visibility of the cyber resilience framework.*

Resources

There are a number of free online resources to help organisations upgrade their cyber resilience capabilities, which we consider useful for small and medium-sized FAPs.

CERT NZ has a number of useful and practical resources for businesses on keeping systems and data safe from cyber security attacks, including cyber security risk assessments for business, cyber security awareness for staff, phishing scams and your business and protecting your business online.

CERT NZ offers the following tips for simple, practical steps for businesses. A detailed version of these tips is available here.

1. Install software updates
2. Implement two-factor authentication (2FA)
3. Back up your data
4. Set up logs
5. Create a plan for when things go wrong
6. Update your default credentials
7. Choose the right cloud services for your business
8. Only collect the data you really need
9. Secure your devices
10. Secure your network
11. Manually check financial details

We encourage FAPs to subscribe to CERT NZ's updates here.

The Institute of Directors New Zealand has published a cyber risk practice guide to help boards understand and approach cybersecurity in their organisations – available here

The National Cyber Security Centre (NCSC) is part of the Government Communications Security Bureau. Its role is to help New Zealand's most significant public and private sector organisations to protect their information systems from advanced cyber-borne threats. They have produced some guidance on cyber resilience that FAPs may find useful – available here.

NCSC United Kingdom has published guidance for self-employed and sole traders here and for small businesses here.

National Institute of Standards and Technology (NIST) provides a cybersecurity framework to assist organisations in planning, prioritising and managing their cyber resilience. It is guidance that can be customised by different sectors and individual organisations to best suit their risks, situations and needs.

'Have I been pwned?' is a free resource that allows anyone to quickly check if they may have been put at risk due to an online account being compromised or "pwned" in a data breach.