FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TĀTAI HOKOHOKO

JUNE 2022

Cyber Security & Operational Systems Resilience

This information sheet assists market services licensees (excluding benchmark administrators) licensed under Part 6 of the Financial Markets Conduct Act 2013 (FMC Act) to enhance the resilience of their cyber and operational systems. While this information sheet is designed to apply to a broad range of sectors, entities with complex cyber security and operational systems should consider the specific technology requirements and obligations that apply to their sector.

Introduction

Cyber attacks affecting New Zealand organisations are increasing in frequency, sophistication and severity. According to the New Zealand National Cyber Security Centre (NCSC), 404 incidents with a national impact were recorded in the year 2020/21, up 15% on the 352 incidents recorded in the previous year.

While such attacks are typically industry and size agnostic, New Zealand's financial services are a popular target, recording the highest number of reported incidents across all industries according to the national Computer Emergency Response Team (CERT NZ) Data Landscape 2022 report, with 91 incidents reported in the quarter ending 31 March 2022.

In light of such increasing cyber threats, technology-related outages and remediation programmes reported to the FMA, it appears that there are shortcomings in the cyber resilience and operational systems at the entities we regulate, including underinvestment in technology and the use of unsupported or legacy systems.

In July 2021, the FMA released a cyber resilience information sheet for financial advice providers (FAPs). While primarily intended to assist small and medium sized FAPs, the FAP cyber resilience information sheet may also be useful for FMC Act licensed entities under Part 6 (excluding benchmark administrators) as it outlines simple actions that entities can take to improve their cyber resilience. Where entities hold both a FAP and another FMC Act Part 6 Licence, the information sheets can be read together. Entities should consider the information provided in light of their size, nature, risk appetite, complexity and specific security

risks, when designing what cyber security and operational systems resilience policies, processes, and controls are appropriate for their organisation.

2019 review of cyber resilience

In 2019, the FMA published a thematic review of cyber resilience in FMA-regulated entities, which utilised the US National Institute of Standards and Technology's (NIST) Cybersecurity Framework, for entities to self-assess their cyber resilience maturity across five core cyber security functions: Identify, Protect, Detect, Respond, and Recover.

Our thematic review found most participants were aware of the increasing cyber security risk and had self-assessed themselves as being highly capable of protecting against, and recovering from, such threats. However, participating entities did not rate themselves highly in terms of detecting and responding to cyber threats. Participants also predicted that their cyber resilience was generally expected to improve over the following two years.

The review highlighted our expectations around cyber and operational resilience and recommended that licensed entities use a recognised cyber security framework, tailored to their organisation, to assist with the planning, managing and prioritisation of cyber resilience. It also highlighted the importance of having an established response and recovery plan in place.

Following the thematic, we expected entities to reflect on our findings and, where necessary, improve their cyber resilience capabilities.

Standard conditions

All FMC Act entities licensed by the FMA under Part 6 (excluding financial advice providers) are subject to a standard condition on compliance, as outlined in the standard conditions for each licence type, requiring them "to have, at all times, adequate and effective systems, policies, processes and controls that are likely to ensure you will meet your market services licensee obligations in an effective manner".

Additionally, to be licensed, all FMC Act Part 6 licensed entities (excluding financial advice providers) must meet the minimum standard for operational infrastructure as outlined in the licensing guide for each licence type. This specifically states that "IT systems used to deliver the licensed market service must be secure and reliable. Your arrangements ensure they perform efficiently and the associated risks are managed".

Based on the above, our expectation is that entities have adequate technology architecture, cyber security systems, processes and controls in place to ensure their technology risks are being managed and their licensed services obligations are continuing to be met. This also includes an expectation that systems processes and controls are tested and assessed on a regular basis to ensure that their data and technology systems are secure and operating effectively.

For FAPs, the FMA's November 2020 'Standard Conditions for full financial advice provider licences' prescribes specific obligations for business continuity and technology systems. The FMA's July 2021 'Developing cyber resilience for financial advice providers' information sheet provides further detail on the FMA's expectations in meeting this obligation.

Future focus on cyber and systems resilience

Given the increasing digitisation of financial services, the growing prevalence of cyber attacks and the increasing numbers of technology incidents reported to the FMA, we have heightened our focus on licensed entities' cyber and operational resilience. As outlined in our annual corporate plan for FY21/22, we will be enhancing our regulatory approach to cyber and operational resilience, including reviewing entity obligations, enhancing our monitoring approach, and engaging with stakeholders and other regulators to raise awareness and capability.

Cyber resilience and operational systems risk management

Part 6 FMC Act licensed entities (excluding benchmark administrators) should have effective cyber security and operational systems resilience controls, processes, policies and people capability in place. This includes being aware of the risks that potentially impact their organisation including supply chain risk and understanding their own capabilities. Entities should have appropriate governance, training, incident response management, reporting and remediation structures in place.

Understanding cyber and technology systems resilience capabilities

On an ongoing basis, entities should take steps to understand and regularly review their cyber resilience and technology capabilities in order to identify vulnerabilities specific to their organisation. Cyber security controls, processes and policies should be reviewed, tested and updated frequently, especially in light of any changes in the organisation, or trends in the threat landscape. This will ensure that each entity maintains an appropriate level of information security, technology capability and maturity, in accordance with its risk appetite.

Similar to the self-assessment exercise in the FMA's 2019 thematic, entities can also self-evaluate their cyber resilience against the NIST Cybersecurity Framework functions. This framework recommends that the five NIST functions are reviewed and performed concurrently, in order to form a cycle of continual improvement in cyber resilience. In relation to each of the NIST framework elements, this may include (but is not limited to) the following:

- 'Identify':
  - Developing and reviewing an organisation-wide understanding to manage cyber security risk to systems, people (including customers), assets, data, and capabilities.
  - Understanding the business context and resources that support critical functions, and the associated cyber security risk to enable an entity to set its risk appetite and prioritise its activities
- 'Protect':
  - Developing, implementing and testing safeguards to ensure delivery of critical services and support the entity's ability to limit or contain a cyber security incident.
- 'Detect':
  - Developing, implementing and testing activities designed to enable timely identification of the occurrence of a cyber security incident.
- 'Respond':
  - Developing, implementing and testing activities and actions that entities can take upon discovery of a cyber security incident, and support the entity's ability to contain the impact.

- 'Recover':
  - Developing, implementing and testing activities which enable the entity to restore capabilities and/or services that were impacted by a cyber security incident.

Organisations should take steps to understand the maturity and state of their system architecture and technology systems. Organisations should also frequently review their technology and operational systems to identify potential areas of weakness, and to determine if they are fit for purpose. This includes reviewing whether systems and their controls are operating effectively and as intended via testing and quality assurance.

Entities should also consider engaging an independent cyber security or technology specialist to conduct a review which will help them understand their maturity level and identify key points of vulnerability unique to the organisation. This would be a particularly useful exercise for entities without in-house cyber security or technology specialists as it will provide them with a specialised and objective view.

Engaging a cyber security specialist to conduct a penetration test, or performing crisis management simulations may also be useful, as they will test whether the entity's controls, policies and processes are able to withstand a security incident.

The Reserve Bank of New Zealand's Guidance on Cyber Resilience also provides a helpful framework for entities that are reviewing and tailoring their cyber resilience controls, processes and policies to meet their technological needs and risk appetite.

CERT NZ's Critical Controls is another useful resource for entities and their IT professionals. It provides a list of 10 measures which provide the highest degree of protection against common cyber security attacks. Similarly CERT NZ's Top 11 Tips for Business also provides a list of practical steps for entities to help protect against cyber attacks.

Understanding the threat landscape and key risks

Given the rapidly changing cyber security threat landscape, entities licensed under Part 6 of the FMC Act (excluding benchmark administrators) should be aware of risks that impact their organisation, and must react and adapt accordingly. Entities should be continually scanning the threat landscape to identify potential risks to their organisation and customers. Similarly, entities should monitor for any alerts that may critically impact their service providers.

Entities can stay up-to-date with potential and upcoming cyber security threats by subscribing to CERT NZ's alerts and advisories.

Supply chain risk

While entities may review and consider cyber security and the resilience of operational systems within their organisation, the same focus and scrutiny is often not applied to their supply chains and third-party vendors. With bad actors more frequently targeting service providers, the risk to supply chains increases.

Entities should frequently review their supply chains and outsource providers to assess their criticality. This involves identifying key services and assets which, if compromised, would cause significant risk or disruption to the business and its activities. Entities should also consider if the information held or processed by outsource providers is confidential or sensitive.

Once critical assets and services have been identified, any associated risks can also be assessed. Processes and controls to mitigate the risk of an incident, such as contingency plans, can then be built around the criticality of each asset.

The Outsourcing standard condition for FMC Act Part 6 licensed entities states that entities must be satisfied "that the provider is capable of performing the service to the standard required". As such, entities should take measures to understand their suppliers' security measures and standards, and to communicate their expectations and cyber security requirements to meet their needs. Reviews of outsourced or third-party vendors should also consider whether the entity's technology needs and cyber security expectations are continuing to be met.

The NCSC has published helpful guidance on supply chain cyber security which includes information on how entities should review their supply chains, and how they can establish a programme for managing cyber risk within supply chains.

Governance

As cyber security threats impact all levels within an organisation, boards and senior management should have a strong understanding of the state of their operational systems and technology, and the cyber risks facing their organisation. Boards should have a heightened focus on technology risk as they are ultimately accountable for cyber and technology risk management and strategy, and because the loss associated with a technology incident can be severe, e.g. loss of sensitive or confidential business and customer information, reputational loss and financial loss.

Boards should make an ongoing commitment to improving cyber and technology resilience within their organisation. Where uplift or remediation is required, boards should ensure there is sufficient capability and resourcing available. Senior leadership should also be responsible for cultivating a culture of cyber security and technology risk awareness within the organisation.

New Zealand's Institute of Directors provides a number of helpful resources to help boards understand privacy principles, and cyber risk and resilience . The NCSC also provides helpful guidance to business leaders to enhance their cyber security governance.

Training

As cyber risk exists within all levels of an organisation, cyber security awareness training should be provided to all staff. Employees should be regularly trained on the importance of cyber security, the potential threats to their organisation, the reality of cyber attacks and how to respond to a potential compromise.

Role-specific training should also be provided to staff in higher risk roles, such as those with higher security or access permissions. CERT NZ provides useful tips on how organisations can build cyber security awareness within their business.

Incident response and management

FMC Act Part 6 licensed entities (excluding benchmark administrators) should have a key focus on preventing cyber attacks and mitigating technology incidents, and be able to demonstrate this by having effective key controls, governance, processes, reporting and frameworks in place.

Entities should have established plans, with clear roles and accountabilities, to help ensure they can resume operations without undue delay. When responding to an incident, entities should immediately enact their business continuity and incident management plans. These plans should also include an approach for informing and remediating customers. Business continuity and incident management plans should be reviewed, tested and updated on a regular basis, so they are up to date and can be immediately implemented in the event of an incident.

The NCSC provides useful guidance on incident management, including steps on establishing a framework for incident response and management. CERT NZ also provides helpful guidance on responding to cyber security incidents and breaches.

Reporting

Entities should notify the FMA of any technological or cyber security event that materially disrupts or affects the provision of their regulated services, or has a material adverse impact on one or more customers. For example, a report of a phishing campaign affecting staff should not be reported to the FMA, however the FMA should be notified if that phishing campaign is successful, i.e. has resulted in the compromise of data or sensitive information, or financial loss.

The notification should include (but not be limited to):

- current status (ongoing, resolved etc)
- business impact
- customer impact
- affected systems
- severity classification
- projected recovery timelines

The notification should be provided to the FMA as soon as practicable. Where the incident is ongoing, the FMA should be kept up to date on status and recovery timelines until the incident has been resolved.

Entities must ensure they comply with all other legal and regulatory obligations relating to such incidents, including reporting obligations required by other regulators. We also encourage reporting cyber incidents to CERT NZ, which can provide advice and guidance on recovering from an incident, and measures to prevent a future occurrence.

Remediation

Entities should have established incident management plans which include approaches to them informing, remediating and supporting customers in the event of an incident.

Where the incident has resulted in the disclosure of personal information, as defined by the Privacy Act 2020, entities should be aware of their obligations under that Act. The Office of the Privacy Commissioner has published guidance on responding to privacy breaches.

Should customers be affected by a service issue or outage, entities should facilitate the best possible outcomes for affected customers.

Communications regarding the incident should clearly explain the issue to the customer, how they can seek further information, and the complaints process. If applicable, details of any compensation should also be provided. If an action or response is required, this should be clearly outlined and easy to follow.

Where customers have experienced a loss, entities should be able to demonstrate a customer-centric lens and take all reasonable steps to support affected customers. Entities should put customers right and ensure that they are returned to the same state as had the incident not occurred, or as close as possible to that state.

Post incident reporting

Once an incident has been contained and resolved, entities should conduct a comprehensive inquiry to understand the root cause. A post-incident report (PIR) should be provided to the FMA (separate from the initial notification) as soon as practicable after the entity has resolved the incident.

The PIR should include (but not be limited to):

- a comprehensive analysis of the root cause of the incident
- how the entity has rectified or resolved the incident
- accountabilities and responsibilities relating to the incident
- impacts to the entity's cyber security risk profile
- a full assessment of the incident's impact on the business and customers
- key learnings and measures taken by the entity to prevent the incident occurring again.

Timelines and the progress of the remediation, including any customer remediation, should also be reported to the FMA.

Entities may consider engaging a third party to conduct an independent review to ascertain the cause of the incident, especially where technology and cyber capability is not available within the organisation.