FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TATAI HOKOHOKO - NEW ZEALAND

July 2019

Cyber-resilience in FMA-regulated financial services

This report summarises the findings of our thematic review of cyber-resilience in New Zealand financial services, and provides guidance for firms in areas where we have identified the need for improvement. It will be useful for our regulated sectors, to help ensure they comply with our expectations and best practice.

Why are we interested in cyber-resilience?

The operation of financial service firms and financial markets is increasingly digitised, and the incidence and cost of successful cybercrime-related attacks continues to grow.

Cyber-risk encompasses all risk of loss, disruption, or damage to a firm caused by failure in its information technology systems – from both internal and external threats. The interconnectedness of the financial sector means any part of it might be an entry point for a wider cyber-incident.

As part of the FMA's role in promoting fair, efficient and transparent markets, we want to ensure financial service providers and consumers are aware of and prepared for cyber-risks, and that providers have proportionate controls to mitigate risks and ensure cyber-resilience.

Cyber-resilience is already something we look at as part of our regular monitoring of regulated entities. However, we want to develop our monitoring approach to align with the increasing risk and complexity in this area.

To help us understand the current state of cyber-resilience and develop our approach, we conducted a survey of market participants' current cyber-resilience and future plans. The insights developed from the survey have enabled this guidance to be produced and will inform individual FMA support and monitoring activity.

We wish to thank participants who voluntarily took part in the survey. Participants can obtain an individual survey summary from the FMA.

Key recommendations for market participants

All firms should make use of the services provided by CERT NZ, which monitors cyber-incidents and provides advice and alerts, and New Zealand's National Cyber Security Centre (NCSC), which helps organisations protect their systems from cyber-threats.

Market participants should include assessment of cyber-risk – both for their own firm and on a broader global level – as part of their wider risk-assessment and -management programme. They should also consider the types of attacks reported by survey participants and areas subsequently identified for change (see pages 3-4).

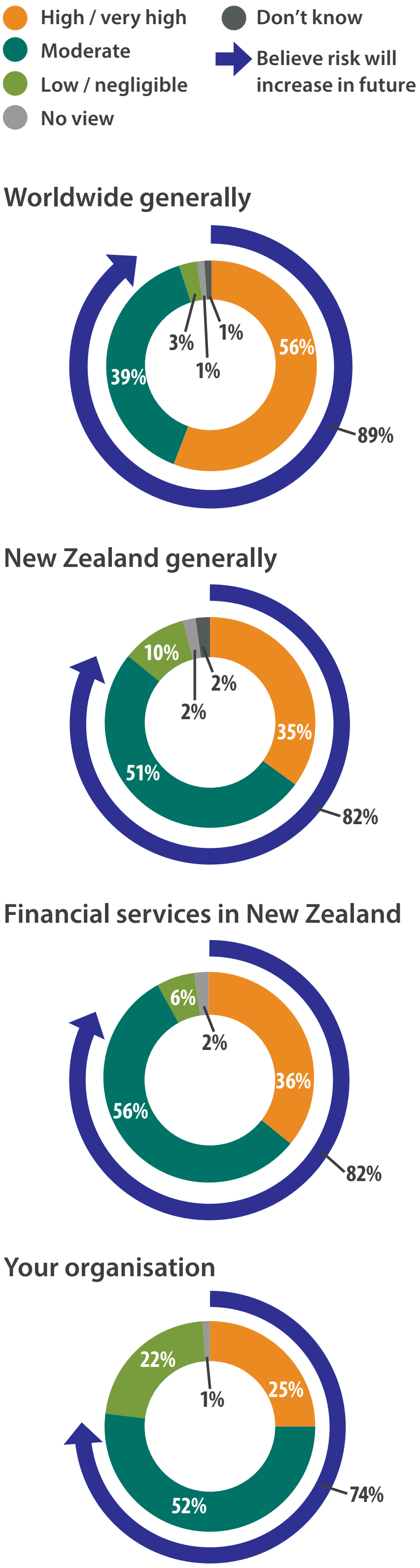
We also strongly encourage all market participants to use a recognised cybersecurity framework to assist with planning, prioritising and managing their cyber-resilience. The National Institute of Standards and Technology (NIST) cybersecurity framework core, for example, enables firms to assess maturity across five functions: Identify, Protect, Detect, Respond, and Recover.

We expect all market participants to have an appropriate balance between protection and detection measures, avoiding over-reliance on protection measures alone. Further, all market participants must have, at a minimum, basic response and recovery plans in place in respect of their regulated service, appropriate to their circumstances.

Firms' governance arrangements must include board and/or senior management ownership and visibility of the cyber-resilience framework. The Institute of Directors' Cyber-Risk Practice Guide provides principles to help boards understand cyber-risk.

Perceptions of risk

Level of cyber-risk



The majority of participants are aware of the high and increasing level of cyber-risk globally – 56% rated the risk as ‘high / very high’, and 89% believe it will increase in future.

However, the level of ‘high / very high’ risk ratings drops to 36% for New Zealand financial services. This drops further to 25% when participants considered just their own firm.

The proportion of participants that rate cyber-risk levels as ‘low / negligible’ increases significantly when moving from a global view through to New Zealand financial services and ultimately to their own firm – where just over one in five hold the view that their level of cyber-risk is low. We also note that, even though all participants are part of the New Zealand financial services sector, 27% rated the cyber-risk level for their own firm lower than the cyber-risk level they ascribed to financial services generally in New Zealand.

In a speech to the Aspen Cyber Summit Forum in November 2018, Andrew Hampton, the Director-General of the Government Communications Security Bureau, pointed out that “New Zealand is exposed to the same cyber threats as our partners around the globe, and indeed any other developed nation with well-established infrastructure”, despite being a small island nation that had historically been able to rely on distance as a defence to many harms.

We do not believe that New Zealand firms face a materially lower risk of cyber-attack than firms in other countries. CERT NZ’s 2018 summary threat landscape report shows a 205% increase in reported incidents from 2017. All licensed firms should treat the risk of cyber-attack as real, and plan accordingly.

We are encouraged that the majority of participants (77%) reported a moderate or high level of awareness of cyber-risk facing their firm, which is likely to factor into decisions about improvements to cyber-resilience levels in future.

Market participants should familiarise themselves with the NCSC’s annual cyber-threat reports and CERT NZ’s reports on the New Zealand cyber-threat landscape.

Reported attacks

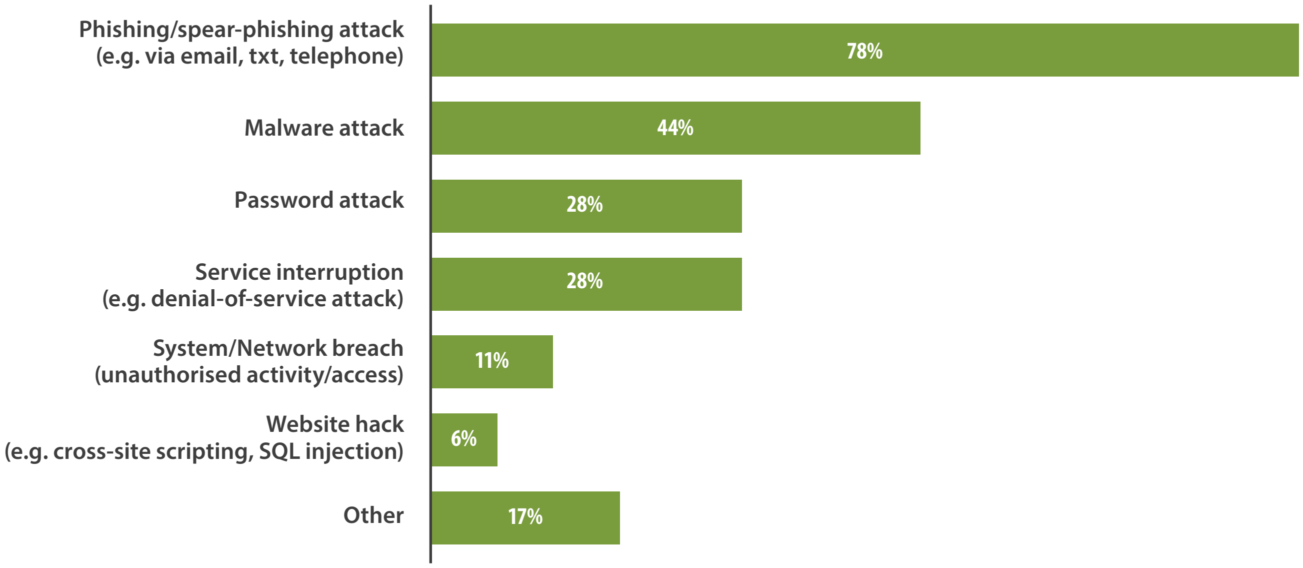
We asked survey participants to provide details of any material cyber-attacks experienced in the prior two years.

Eighteen percent of participants reported experiencing a material cyber-attack, with 9% of participants reporting multiple attacks during the two-year period. With the exception of Authorised Financial Advisers, the reported cyber-attacks occurred at firms of all sizes, across all sectors surveyed. The types of cyber-attacks reported are shown below.

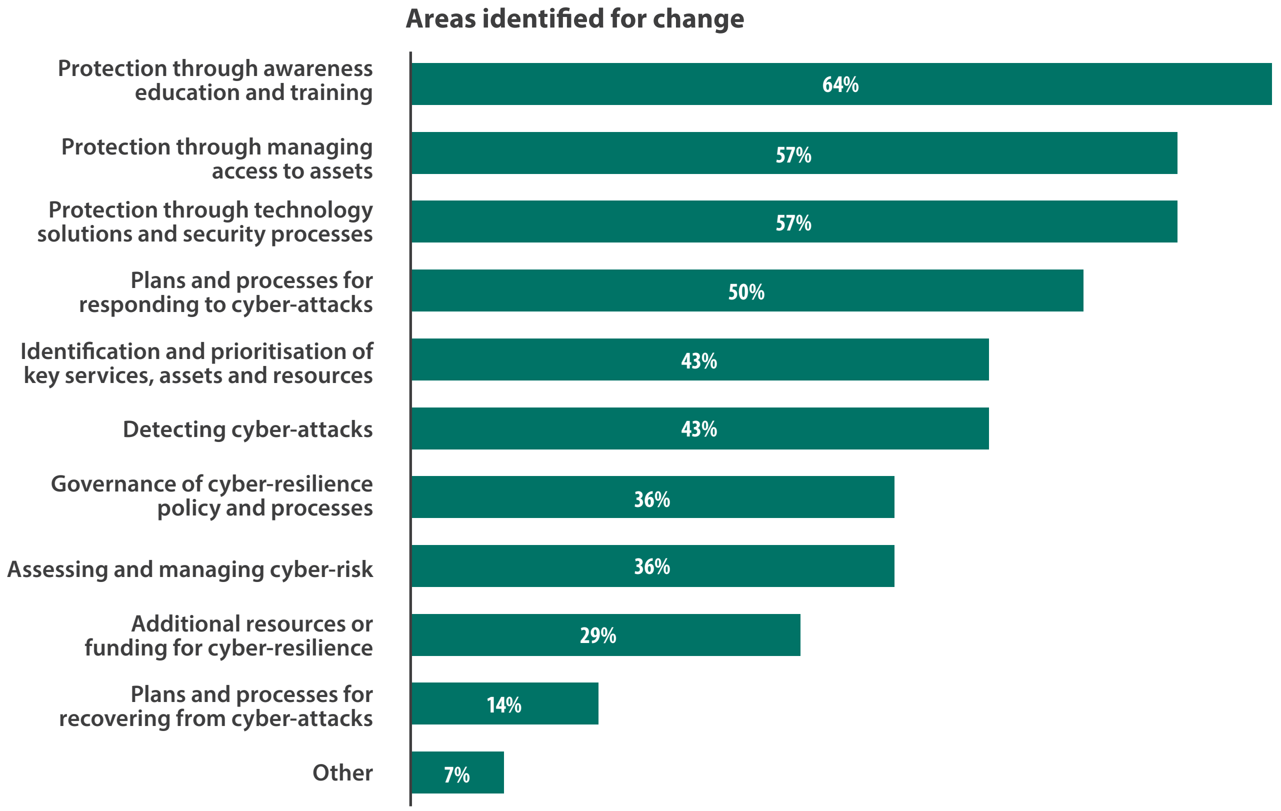
We do not believe that there is any FMA-regulated sector in New Zealand that is 'safe' from cyber-attacks. Financial services firms should not allow their size, or lack of it, to create a false sense of security.

We note that the cyber-resilience 'Detect' capability reported by participants – discussed in the next section – is the lowest-rated component of overall cyber-resilience levels. Therefore it is probable that the actual incidence of cyber-attacks is higher than reported in the survey.

Prevalence of cyber-attack type



Of the firms who reported experiencing material cyber-attacks, 78% identified areas of their cyber-resilience as needing to change. The following are the areas of cyber-resilience identified for change:



It is encouraging that most participants who reported experiencing a material cyber-attack did identify changes to improve their cyber-resilience – all of whom have commenced with this work.

All market participants should consider how these improvements identified as a result of cyber-attacks might apply to their own business.

The remaining 22% of participants who reported cyber-attacks, despite not identifying any necessary changes as a result of experiencing material cyber-attacks in the last two years, are all forecasting material uplifts in cyber-resilience levels within the next one to two years (see page 8). However, we note that the forecast uplift in cyber-resilience is, in most cases, to levels approaching 100%, which we believe is doubtful in such a short period.

Around three-quarters of firms that experienced a material cyber-attack were able to either fully or partially execute an existing plan in response to the attack. Response plans should be a fundamental part of all market participants' cyber-resilience capability – particularly given the weaknesses in the 'Detect' capability that the survey identified.

Firms should subscribe to CERT's free security advisories via email or follow their alerts on Twitter.

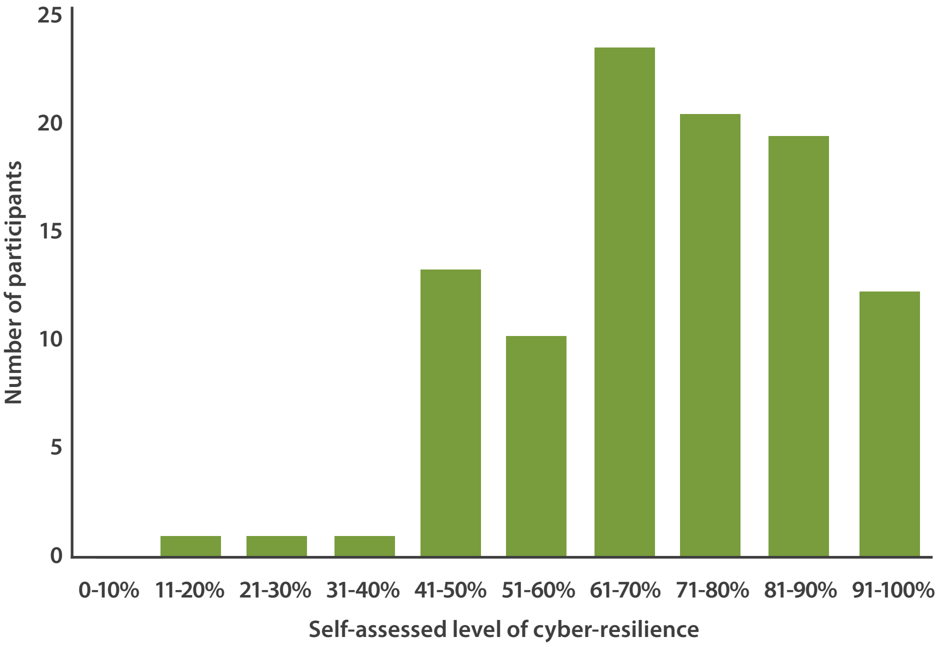
How prepared are participants?

The cyber-resilience topics covered in our survey were based on the NIST cybersecurity framework. The framework groups topics across five functions: Identify, Protect, Detect, Respond, and Recover. Under each function we asked questions about topics related to that function[1].

The findings are based on self-rated responses to each question. Participants were able to respond to any question as 'not applicable' if the topic was not relevant to their particular business model and circumstances, or could respond 'do not know'.

Twelve participants indicated that one or more questions were not applicable to them. Questions with non-rated responses did not negatively affect a participant's cyber-resilience score.

Current overall cyber-resilience levels



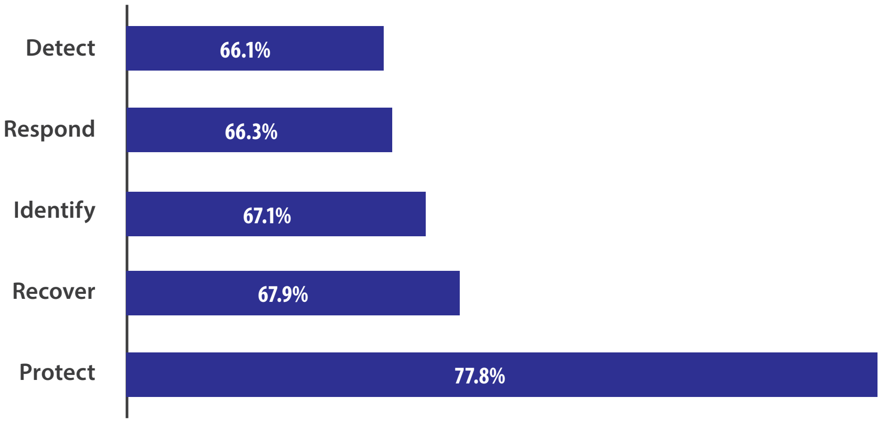
The average self-assessed level of overall cyber-resilience is 70%. Fifty-one of 100 participants rated their overall cyber-resilience level higher than the 70% average, while twelve self-rated at above 90%, including two with a 100% rating. Sixteen participants rated their overall cyber-resilience level at 50% or lower.

The size or financial strength of participants is not related to the level of cyber-resilience. A material number of high-profile financial services firms rated themselves below the average level of cyber-resilience.

The five NIST cybersecurity functions have varying levels of contribution to overall cyber-resilience.

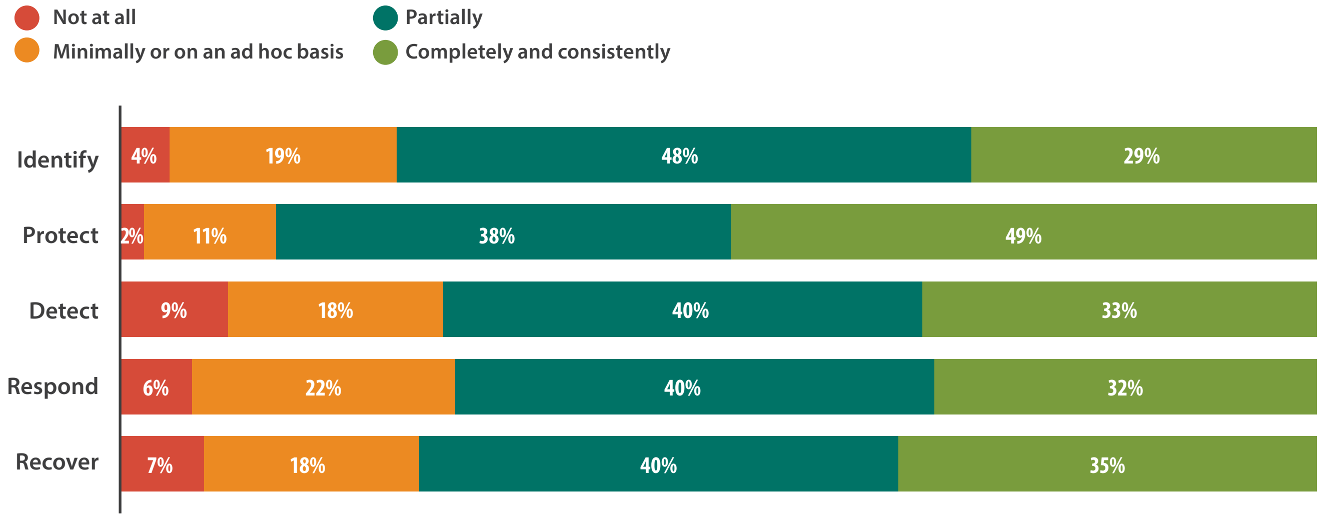
Participants rated their 'Protect' measures the highest, while steps to 'Detect' cyber-attacks and 'Respond' to them are rated the lowest. The 'Identify' function, which informs priorities in the other four functions, is rated in the middle, well below 'Protect'.

Current average cyber-resilience levels by function



[1] The survey covered the 108 NIST topics in 36 questions, using a comparable proportion of survey questions to topics within each of the five NIST functions.

To what extent do participants currently address topics within each NIST function?



Identify

Within the 'Identify' function, it is encouraging that 77% of participants report that individual topics are either partially or completely addressed. Four percent of participants report that no activity is performed for one or more of the topics covered in this function. Overall, determination of organisational cyber-risk tolerance and establishment of cyber-risk management processes have the lowest ratings, followed by the identification of cyber threats and asset vulnerabilities.

Protect

The 'Protect' function has the highest overall rating, with 87% of participants reporting that they either completely or partially address topics in this area. We note that the cyber resilience of participants in the 'Protect' function is based largely on technology-centric measures. Steps to raise cybersecurity awareness through education, and ensuring clarity of cybersecurity roles have the lowest ratings.

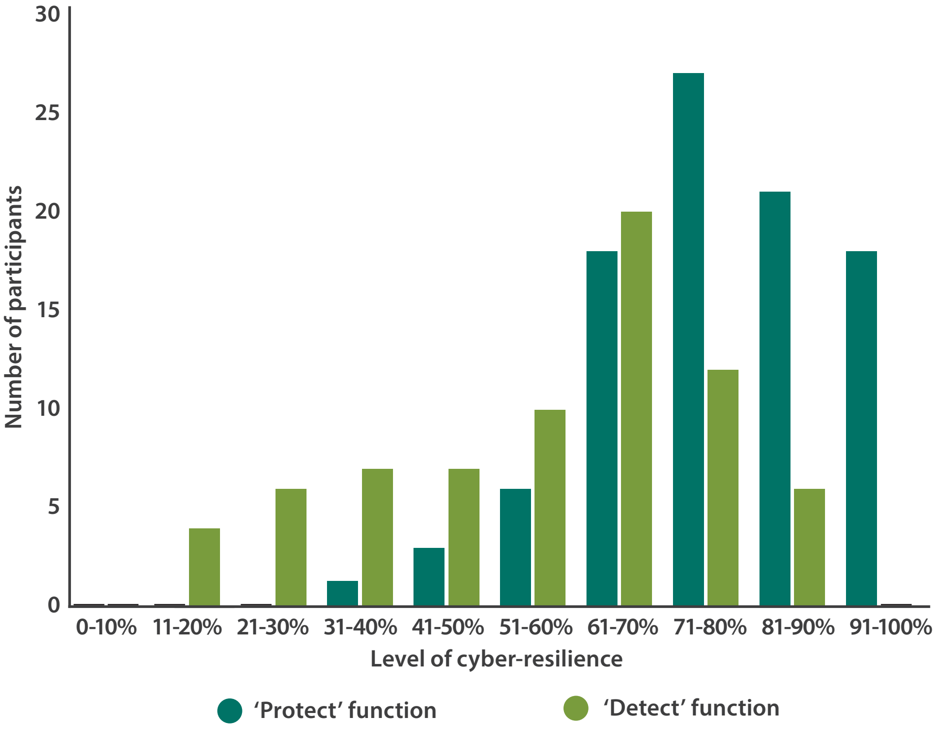
Detect and Respond

The 'Detect' and 'Respond' functions have the lowest overall ratings, with 27% and 28% respectively of participants reporting that no or minimal activity is performed for one or more of the cyber-resilience topics within these functions. Within the 'Detect' function, 9% of participants (the highest of all the functions) report that no activity is performed for one or more of the underlying topics. Within the 'Respond' function, the availability of fully documented and tested response plans (for activation during a cyber-attack) has the lowest rating, with 10% of participants reporting that they do not have a recovery plan at all and a further 28% rating their capability as minimal or ad hoc.

Recover

The 'Recover' function is similar to 'Identify', where 75% of participants report that individual topics are either partially or completely addressed. The availability of fully documented and tested recovery plans has the lowest rating, with 13% percent of participants reporting that they do not have a recovery plan at all, and a further 16% reporting their capability in this area as minimal or ad hoc.

Current cyber-resilience levels for 'Protect' and 'Detect' functions



The material gap between 'Protect' and 'Detect' capability is highlighted in the significantly different distribution of cyber-resilience levels for these two functions (see graph). Participants appear to rely heavily on protective measures, while under-investing in detective measures as part of their overall cyber-resilience.

Similar differences are noted between the distribution of the 'Protect' capability and the distribution of all the other functions.

Future cyber-resilience

Future overall cyber-resilience is forecast to rise from the current average of 70% to an average of 88% within the next one to two years. The range of future cyber-resilience levels is forecast to be between 54% and 100%.

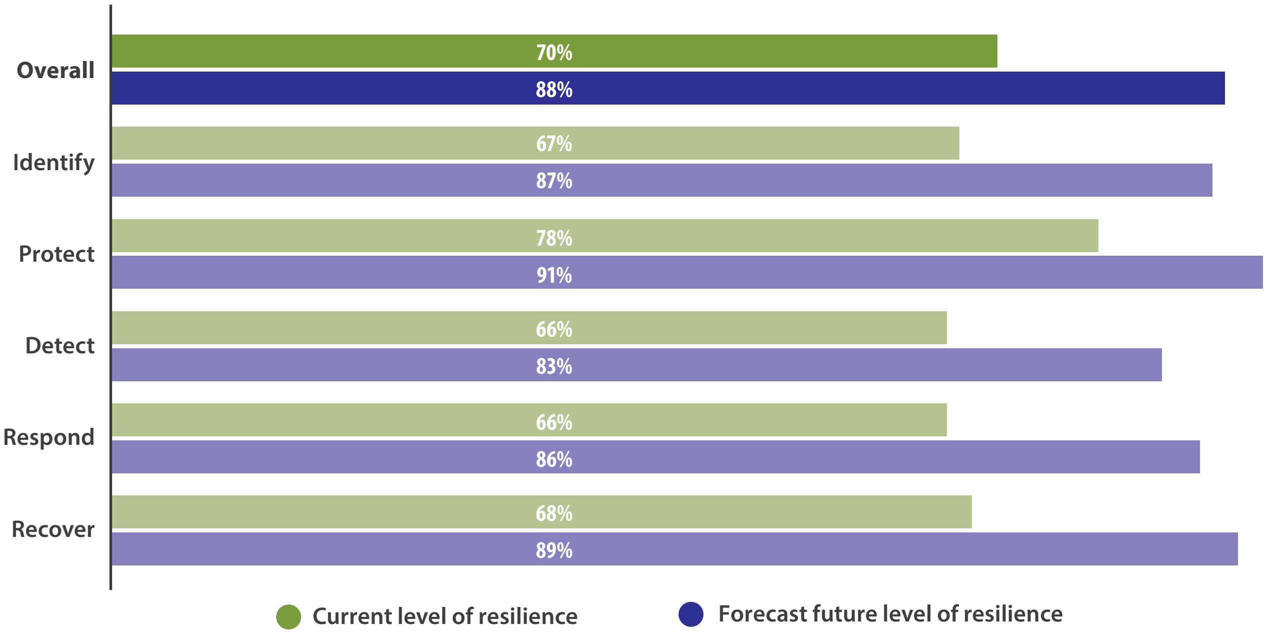
The forecast improvements in cyber-resilience levels are across all the NIST functions, with the 'Protect' function forecast to remain higher than all other functions.

The average forecast uplift in cyber-resilience across all participants is 30.3%.

Participants currently ranked in the top 25 cyber-resilience levels are forecasting an average uplift of 8.5% in the next one to two years, while participants currently ranked in the bottom 25 levels are forecasting an average uplift of 66.1% (with individual forecast uplifts ranging as high as 206%).

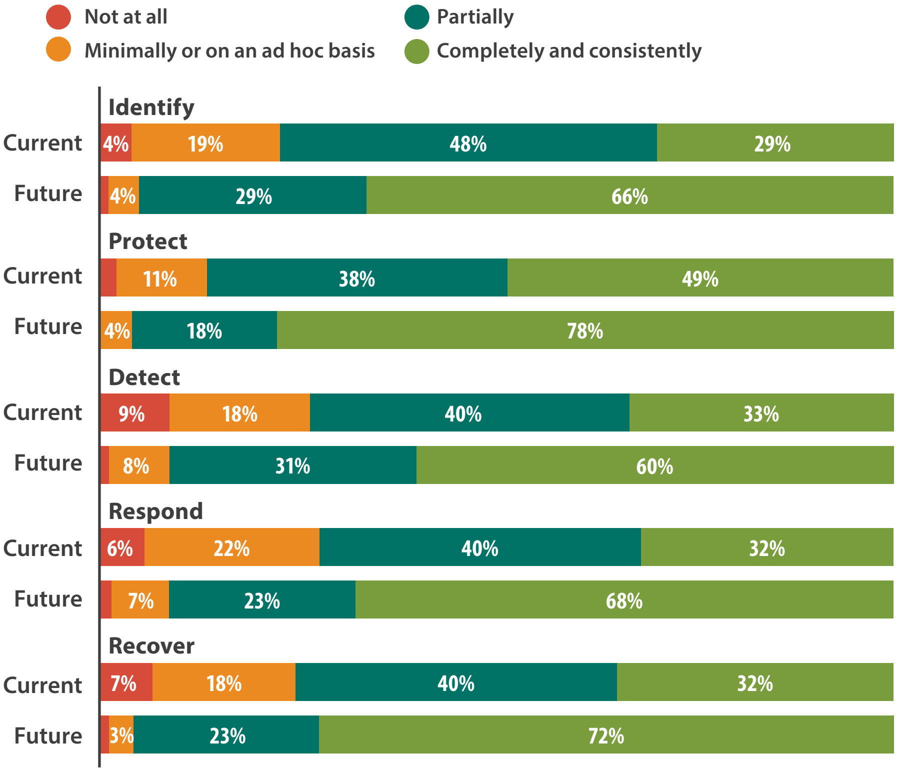
Nine participants are not forecasting an increase in their cyber-resilience level.

Future forecast cyber-resilience levels



The makeup and comparison of current and future ratings within each of the NIST functions is shown below:

To what extent do/will participants address topics within each NIST function?



Many participants could be setting unachievable cyber-resilience uplift targets for themselves, through attempting to substantially improve all aspects of their cyber-resilience within the relatively short period of one to two years.

These participants should review the feasibility of their cyber-resilience improvement plans and use a recognised cybersecurity framework to guide the prioritisation and pace of their cyber-resilience improvements. We believe that this will increase the likelihood of targeted and effective incremental cyber-resilience improvements that are relevant to the circumstances of individual firms.

It is encouraging to see recognition that cyber-resilience levels need to increase across a range of areas. For many participants, there are significant gaps in specific areas that warrant urgent attention and higher priority than other improvements.

At a minimum, we expect all market participants to have basic response and recovery plans in place in respect of their regulated service, appropriate to their individual circumstances. More generally, we expect to see a better balance between protection and detection levels over the next two years.

While large banks reported high levels of cyber-resilience, in keeping with their view of the level of cyber-risk applicable to them, other high-profile firms reported lower-than-average cyber-resilience.

Where FMA has oversight of these firms in conjunction with other regulatory authorities, we will communicate with the relevant authorities to agree any necessary steps. For other situations we will take the survey findings into account as part of ongoing supervision.

Improving cyber-resilience

NIST describes the role of their cybersecurity framework as follows: “The Framework will help an organization to better understand, manage, and reduce its cybersecurity risks. It will assist in determining which activities are most important to assure critical operations and service delivery. An organization can use the Framework to determine activities that are most important to critical service delivery and prioritize expenditures to maximize the impact of the investment.”

All market participants should make use of a recognised cybersecurity framework to assist them in planning, prioritising and managing their cyber-resilience. We do not require the use of any particular cybersecurity framework. However, firms not currently using a recognised framework should consider using the freely available NIST cybersecurity resources. These can be applied to firms of all sizes.

To quote NIST “The Framework should not be implemented as an un-customized checklist or a one-size-fits-all approach. The Framework is guidance. It should be customized by different sectors and individual organizations to best suit their risks, situations, and needs. Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances.”

Participants who make use of the NIST resources should consider using the NIST Framework Implementation Tiers to take stock of their current cyber-resilience activities from an organisation-wide point of view. The tiers characterise a firm’s practices, from Partial (Tier 1) to Risk-informed (Tier 2), Repeatable (Tier 3) and Adaptive (Tier 4). The tiers are not intended to be ‘maturity’ levels, but rather to provide a flexible means of determining if a firm’s cybersecurity risk-management practices are sufficient, taking into consideration its:

- threat environment
- legal and regulatory requirements
- business objectives
- organisational constraints.

Firms should consider progressing to higher tiers when this change would reduce cybersecurity risk and be cost-effective.

The survey findings per NIST function contained in this report do not map directly to the tiers. However, participants should take this report, together with their individual summary, into account when selecting the tiers applicable to them.

Additional resources

Anyone seeking additional cybersecurity information is encouraged to make use of the following resources:

- The National Institute of Standards and Technology provides the NIST cybersecurity framework and related material.
- The International Organisation of Securities Commissions (IOSCO) has published guidance on using standards to address cyber-risk.
- International Organisation for Standardisation (ISO) provides the ISO 27000 standards for information security management.
- The UK Financial Conduct Authority (FCA) has published cybersecurity industry insights.
- ASIC has published an example of how the NIST Framework Implementation Tiers have been used by participants in Australian financial markets.

About the survey

We received responses from 100 participants (91 firms and 9 individuals), representing the following regulated sectors:

- Authorised Financial Advisers
- Crowdfunding platforms
- Derivatives Issuers
- Discretionary Investment Management Services
- Independent trustees (Corporate)
- Managed Investment Scheme managers
- Peer-to-peer lending
- Qualifying Financial Entities
- Supervisors

Banks and insurers were included to the extent they hold licences in these sectors.

AUCKLAND

Level 5, Ernst & Young Building
2 Takutai Square, Britomart
PO Box 106 672, Auckland 1143

Phone: +64 9 300 0400

WELLINGTON

Level 2, 1 Grey Street
PO Box 1179, Wellington 6140

Phone: +64 4 472 9830

FMA
FINANCIAL MARKETS AUTHORITY
TE MANA TATAI HOKOHOKO - NEW ZEALAND