ASIC
Australian Securities & Investments Commission

Cyber resilience of firms in Australia's financial markets

November 2017

This is ASIC Report 555

Disclaimer

This report does not constitute legal advice. We encourage you to seek your own professional advice to find out how the Corporations Act and other applicable laws apply to you, as it is your responsibility to determine your obligations.

Examples in this report are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

Overview

Cyber resilience is vital to all organisations operating in the digital economy, and nowhere is this more important than the financial markets sector, where the trust between an organisation and its clients is essential to its future.

Over the past 24 months, 101 firms across the financial markets sector completed a self-assessment survey on their cyber resilience.

The results of these surveys show that while firms are getting better at managing cyber risk, there's still work to do.

Encouraging progress

Understanding the cyber threat landscape and making effective risk-based investments is a continuous improvement process.

Large organisations with access to specialist skills and resources demonstrate a relatively high degree of cyber resilience compared to small and medium-sized enterprises (SMEs) – some of which are just beginning to develop their cyber resilience.

While there is opportunity for improvement across the entire sector, this is particularly true for SMEs.

74% of organisations have well-managed IT security processes and procedures

66% of organisations reported they have cyber incident response plans in place

What's next?

There is increasing recognition in the industry that cyber security is a strategic, enterprise-wide issue and that investment in cyber risk management is a priority.

Firms are prioritising investment based on their individual assessments of cyber risk. Over the next 12–18 months we are expecting to see a significant increase in cyber resilience across the financial markets sector.

ASIC will ...

Raise awareness

of cyber risk across the financial markets sector by providing good practice guidance and key questions for boards

Measure and assess

the level of cyber resilience in financial markets

Engage and collaborate

with regulated firms

Conduct one-on-one conversations

with firms that appear to be challenged

Review progress

made by firms against their target maturity

About the survey

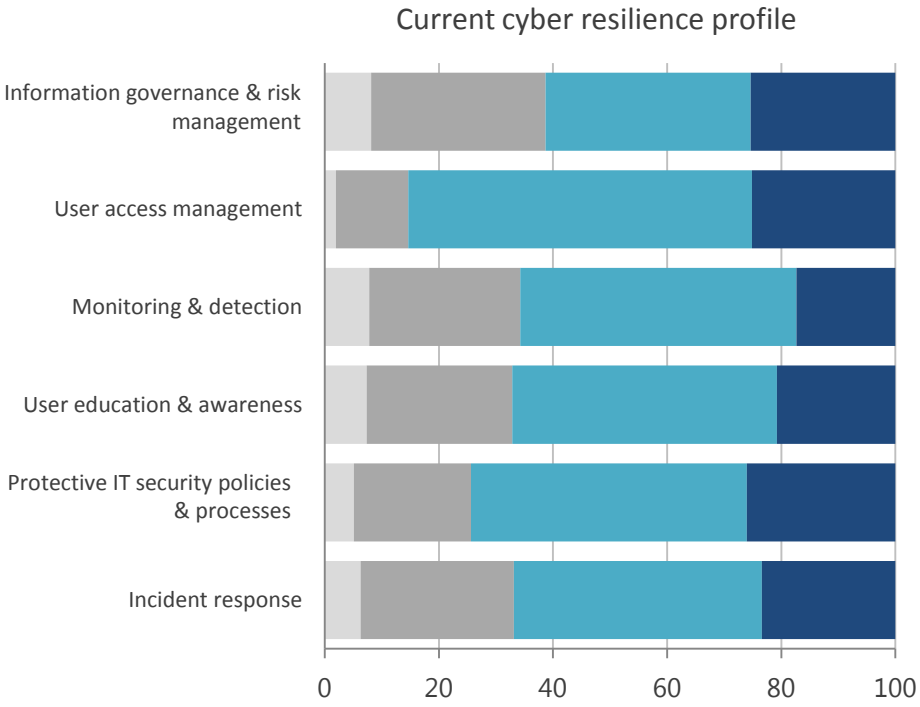
Survey participants were made up of a cross-section of organisations in Australia's financial markets, including stockbrokers, investment banks, market licensees, post-trade infrastructure providers and credit ratings agencies.

Twenty-nine **large firms** provided answers to the National Institute of Standards in Technology Cybersecurity Framework. Seventy-two **SMEs** answered the UK Cyber Essentials.

Using the surveys, firms assessed themselves against six cyber resilience categories using a maturity scale of where they are now (current) and where they intend to be in 12–18 months' time (target).

The cyber resilience categories included information governance and risk management, user access management, monitoring and detection, user education and awareness, protective IT security policies and processes, and incident response.

Note: ASX Group and Chi-X were formally assessed by ASIC in 2016, these results have been included in this analysis.



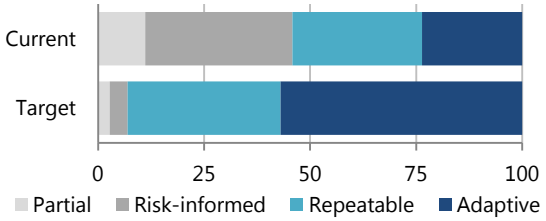
Cyber resilience maturity scale

Cyber resilience of SMEs

Information governance & risk management

Effective information risk management requires formal governance, policies and procedures. SMEs have found information risk management challenging with almost half reporting that they are currently at 'partial' or 'risk-informed' maturity – indicating significant room for improvement. However, they are targeting a 39% improvement in the next 12–18 months, which would leave only 7% as 'partial' or 'risk informed'.

> "whilst there are procedures in place for cyber risk management, it has been recognised that these need to be documented, approved formally and reviewed regularly" – **[Partial]**
>
> *Retail stockbroker*

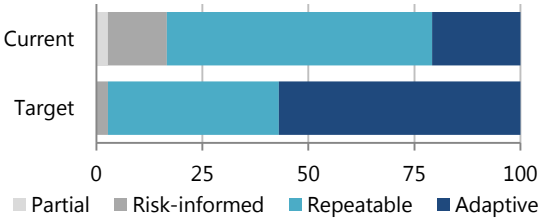


User access management

User access management is the strongest area for SMEs with 83% reporting current maturity as 'repeatable' or 'adaptive'. Ninety-seven percent reported a target of 'repeatable' or 'adaptive' over the next 12–18 months, which would leave only 3% at 'risk-informed'.

A common principle identified in many responses is the use of 'least privilege' (i.e. users are given the least amount of access necessary to perform their business role). This appears to be the standard for many SMEs. While some common themes were identified, it is clear that SMEs are operating at a wide range of maturity levels.

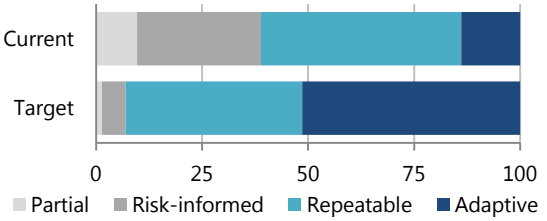
More mature organisations reported that user access is managed by senior personnel and is regularly updated. Others noted that user access is 'not documented or formally approved'.



Monitoring & detection

Almost 40% of SMEs reported shortcomings in monitoring and detection practices. However, they are targeting a 32% improvement in the next 12–18 months, which would leave only 7% with low maturity levels.

One firm stated that there was 'no formal policy' in this area. They went on to explain that 'the network is not a managed network where active monitoring could be implemented at the ISP layer' but that it is 'in place at the network level'. This demonstrates an understanding of the area even though no formal policies are in place. The next step for this organisation – like many other SMEs – is to review and formalise these policies.



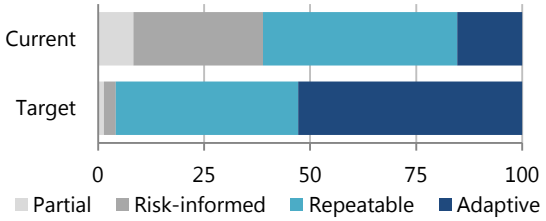
Cyber resilience of SMEs

User education & awareness

User education and awareness is another area that requires work by SMEs. Currently, only 61% of SMEs are at 'repeatable' or 'adaptive' maturity in this area. While this number is far too low, it is encouraging to see a targeted improvement of 35% – which would leave only 4% of SMEs at 'partial' or 'risk-informed' maturity.

> "users have been educated on a casual and ad-hoc basis. A more formal and comprehensive education regime is being developed" – **[Risk-Informed]**
>
> *Proprietary trader*

There are clear differences between well-managed and less mature SMEs in this area. Some of the more mature SMEs identify user education as a 'top priority', referencing 'frequent trainings'. Less mature SMEs have a tendency towards training that is often provided on an 'informal' or 'ad-hoc' basis.

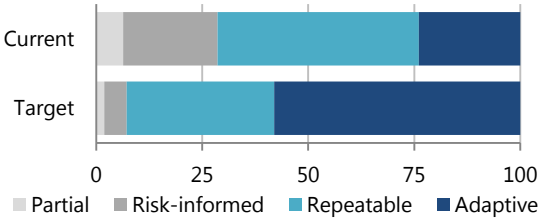


Protective IT security policies & processes

Protective IT security policies and processes are a relatively strong area for SMEs, although there is still room for improvement. Currently, 71% of SMEs are at 'repeatable' or 'adaptive' maturity in this area, with targets of 93%.

Over 80% of SMEs reported that security management of servers, networks, and security testing was well managed – with plans to improve this to 95% within the next assessment period.

However, substantial improvement is required around mobile security and removable media – where 40% of SMEs reported a 'partial' or 'risk-informed' maturity level for both areas. While improvements in mobile security are set at a healthy target of 35%, targeted improvements for removable media controls need to be improved.

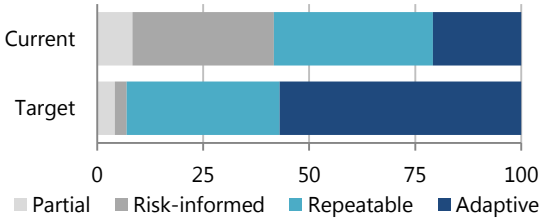


Incident response

Significant improvements are required around incident response management. More than 40% of firms are currently at 'partial' or 'risk-informed' maturity. The common theme is a lack of formalised processes.

SMEs acknowledge the importance of this area and are targeting a 35% improvement, which would leave less than 10% as 'partial' or 'risk-informed'.

> "No incident response plan exists for a cyber security breach. A related entity in the group recently experienced a denial of service attack. We are developing a framework from that experience, having worked through the issue with CERT Australia" – **[Partial]**
>
> *Retail stockbroker*



Cyber resilience of large firms

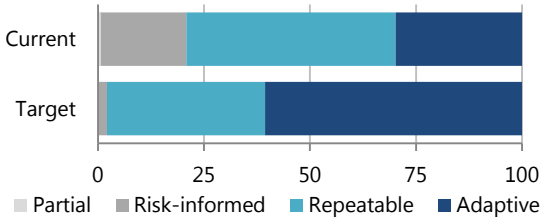
Information governance & risk management

All large firms understand their regulatory cyber security obligations and have information and cyber security policies in place which are communicated across the organisation and periodically reviewed and updated.

Forty-one percent of firms indicated that a proper understanding of information flows across the organisation was a work in progress. Forty-five percent are still grappling with their understanding of externally managed systems and data. All firms indicated that these were priority areas for the next investment period.

Areas of improvement include:

- receiving and sharing threat information from external sources
- identification and prioritisation of asset vulnerabilities and risk responses.



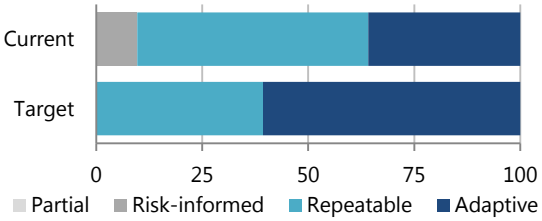
User access management

User access control is well managed by large firms. For example, user access to systems and data is permissions-based and physical access to assets is controlled.

> "[Firm] has a number of published and approved policies and procedures regarding access control" – **[Repeatable]**
>
> *Credit rating agency*

Senior management generally understand the threat landscape, and their roles and responsibilities within their organisation. Users that have 'privileged' access to systems usually have a clear understanding of their cyber security roles.

Ensuring third parties understand their cyber security roles as part of the supply chain is more challenging (e.g. 10% were 'partial' and 17% were 'risk-informed'). While there is a strong appetite to improve status, 3% indicated they would aim to remain at 'partial' by the end of the next investment period.



Monitoring & detection

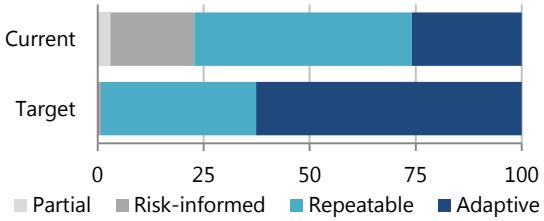
Large firms generally demonstrate a high level of maturity around the monitoring of activities on networks. This includes detection and management of malicious software and anomalous user activity.

> "External penetration tests ... are conducted every 6 months and internal penetration tests once every 12 months by a 3rd party vendor. Results from the penetration tests are remediated using a formal process" – **[Repeatable]**
>
> *Australian market licensee*

Monitoring of unauthorised mobile software is still an issue despite efforts to reduce risks.

Areas of improvement include:

- establishing baselines for expected information flows over networks to allow anomalies to be detected
- aggregation of multiple information sources to improve threat detection and assessment.



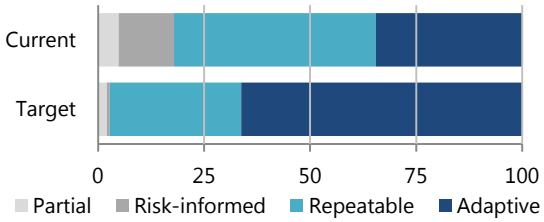
Cyber resilience of large firms

User education & awareness

User education and awareness remains high on the agenda for all large organisations, particularly for the 21% that are currently 'partial' or 'risk-informed'. All firms indicated that they plan to prioritise user training and awareness going forward.

"[Firm] has a Security awareness program that includes mandatory 20 minute annual training. Year around reinforcement includes videos, monthly phishing simulations, intranet content" – **[Adaptive]**

Credit rating agency



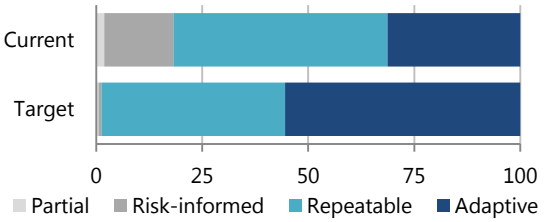
Protective IT security policies & processes

There has been a shift in the way data protection technology is being applied. For example, there is increasing use of data encryption for data that is stored and transmitted over networks.

Sixty-two percent of organisations indicated that they intend to improve their data protection arrangements in the next 12–18 months.

"Removable media guidelines are provided and enforced through IT Use Policy" – **[Repeatable]**

Credit rating agency



Incident response

Significant improvements are required around incident response management. More than 40% of large firms are currently at 'partial' or 'risk-informed' maturity. The common theme is a lack of formalised processes.

Firms acknowledge the importance of adequate incident response management and are targeting a 35% improvement. This would leave less than 10% of large entities as 'partial' or 'risk-informed'.