FINANCIAL CONDUCT AUTHORITY

Cyber and Technology Resilience: Themes from cross-sector survey 2017 - 2018

November 2018

Cyber and Technology Resilience: Themes from cross-sector survey 2017 - 2018

Contents

1. Introduction

1.1. Technology plays a pivotal and often innovative role in delivering and improving financial products and services to markets and customers. However, it can also lead to harm if not effectively managed or kept secure.

1.2. To gain a better understanding of the industry's resilience we surveyed 296 firms during 2017 and 2018 to assess their technology and cyber capabilities. The survey looked at key areas such as governance, delivery of change management, managing third party risks and effective cyber defences. Firms self-assessed their capabilities and the FCA then analysed the responses for each firm and across sectors.

1.3. This report highlights the key themes from the self-assessment alongside data about the operational incidents firms have reported to the FCA. The report identifies areas of strength and those for improvement across all sectors.

1.4. This report is relevant for all firms whatever their size. We draw out the different responses from large and smaller firms and we encourage all firms to consider how our findings apply to them.

1.5. In July 2018, we published a joint Discussion Paper on building the UK financial sector's operational resilience with the Bank of England and Prudential Regulation Authority. This report supports this wider work on operational resilience and the UK's national cyber security strategy.

2. Executive summary

2.1. Operational resilience is a vital part of protecting the UK's financial system, institutions and consumers, as recent disruptive events illustrate. Cyber-attacks show no sign of decreasing in volume. They accounted for 18% of the operational incidents reported to the FCA between October 2017 and September 2018.

2.2. Technology outages in the financial services sector are becoming more frequent and publicised. The number of incidents reported to the FCA has increased by 138% in the past year[1]. Technology continues to evolve rapidly with firms looking to take advantage of this innovation, while sometimes still relying on ageing IT systems.

2.3. Firms identified **governance** as the area where they have the strongest capability. In both our technology and cyber surveys 90% of firms assessed themselves as having strong governance controls. Firms that are subject to the Senior Managers Regime often reported a clearer structuring of roles and responsibilities and ownership of a cyber security strategy. However, some larger firms identified a lack of cyber and technology knowledge at board level, which may limit the effectiveness of board challenge. Board and senior management engagement with cyber and technology resilience is critical to improving firms' wider operational resilience.

2.4. Most firms rank **cyber** resilience as their top concern. Firms' responses highlight cyber weaknesses in 3 areas: **people, third party management,** and **protecting their key assets**. Nearly 80% of respondents struggle to maintain a view of what information they hold[2] and of their third parties. Firms also identified challenges in identifying and managing their high-risk staff and then educating those employees with access to critical systems or sensitive data, who are more likely to be targeted by cyber criminals.

2.5. There is scope for improving **information sharing**. We are encouraged that many larger firms play active roles in information sharing networks and platforms. However, we are concerned that this does not extend to smaller firms. Many small firms felt they did not have anything relevant to share. This may mean that valuable information is missing from these forums.

2.6. Many firms reported that they have mature IT **change management** functions. This is unsurprising given the amount of change many firms undertake. However, failed IT changes caused 20% of the operational incidents reported to the FCA, between October 2017 and September 2018.

2.7. Firms also describe challenges in **managing their third parties**. Third party issues, such as an IT failure at an important supplier, accounted for 15% of the operational incidents reported to the FCA (the second highest root cause). This demonstrates how increasingly important third parties are to firms and their customers, and the need to manage them effectively to prevent disruption.

---

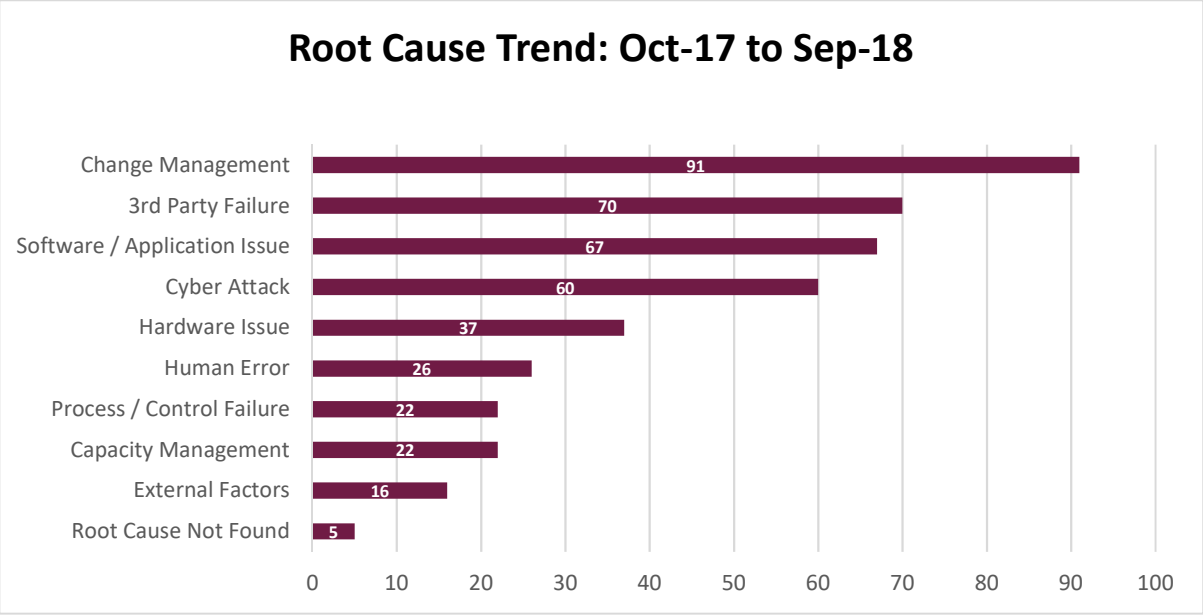
[1] Between the year ending September 2017 and the same period in 2017/18

[2] The FSB Cyber Lexicon defines Information Assets as 'something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation' http://www.fsb.org/2018/11/fsb-publishes-cyber-lexicon/

2.8. Across all firms' cyber resilience responses, retail banks and non-bank payments firms self-assessed as having the most mature capabilities across almost all areas. This may, in part, reflect that firms in these sectors are more regular targets for cyber-attacks. This provides them with experience and relevant intelligence, but also highlights the need for heightened capabilities among these firms. Their relatively stronger self-assessed scores are not grounds for complacency. These firms often have relatively complex IT estates, which inherently increases vulnerability to attack.

2.9. In other sectors, including wholesale markets and retail lending, there was a wide range of scores. Some assessed themselves as very mature and others as much weaker. Retail lending and retail investment firms' survey responses indicate they recognise they have significant room for improvement across both cyber and technology resilience.

2.10. In this report, we compare incident data reported to the FCA to firms' responses to the survey. Under Principle 11, we expect firms to **report major technology outages and cyber-attacks** to the FCA. Evidence suggests that firms are under reporting and we remind all firms of their obligations to report. Firms that are subject to the second payment services directive should comply with the major incident reporting guidelines that form part of this directive. Our cyber resilience web pages and our 'Good Cyber Security - the foundations' infographic set out details of how and when a cyber incident should be reported. The graph below shows the known root causes of the issues reported to us over the past year.



Note: There are 186 cases (29% of total incidents) where firms have not yet informed us of the specific root cause of the incident. We remain in discussions with relevant firms to obtain this information.

3. Key themes

Governance

3.1. Firms assessed governance as the area where they have the most mature capabilities. This was true across both the cyber and technology resilience questionnaires. However, there are areas for improvement including senior level engagement, challenge and skills.

3.2. Identifying clear accountabilities is more of a challenge for smaller firms. Sixteen percent said they lacked a nominated individual at Board or senior level with responsibility for technology resilience. Twenty percent of smaller firms did not have an overall technology strategy approved by the board and 26% did not have a board-approved information security strategy.

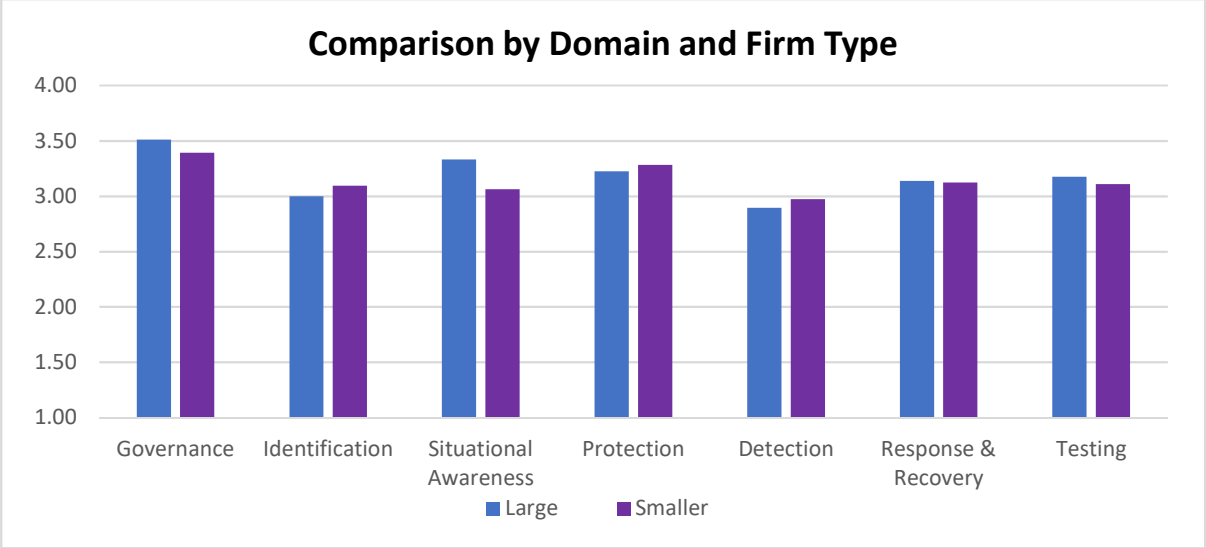
3.3. In contrast, those firms which are subject to the Senior Managers Regime often reported a clearer structuring of roles and responsibilities and ownership of a cyber security strategy. Effective governance at senior levels is essential to creating an environment for effective resilience throughout an organisation, whatever its size.

3.4. Smaller firms, or those with a large presence in other jurisdictions, called out challenges in how a cyber strategy is set and its subsequent board ownership. For example, more complex or geographically diverse firms were more likely to rely on committees and other parts of their groups, with decreasing ownership at board level. Smaller firms often described their cyber strategy as incomplete or as not having been implemented.

3.5. Firms also reported a lack of Board understanding of cyber risks. Additionally, management information is often not presented to the Board in a way that can be easily understood and challenged. We have also seen this in our supervisory work. Some Boards struggle to understand that cyber is a global risk not just the responsibility of the IT department. To mitigate this risk some firms use training and simulation exercises to strengthen their capabilities and others have hired third party firms or advisors. Bringing in external support is one way in which firms can address this challenge. However, this can lead to over-reliance, which in turn could impact the development of their own in-house capabilities.

Cyber resilience

3.6. Firms assessed themselves as having effective cyber controls. However, there are notable exceptions within some sectors and some domains. The areas seen by firms as requiring the most improvement were **identification** of key assets, services and people, including those provided by third parties, **sharing information** and **detection** of attacks.



Note: For each question firms assessed themselves on a range from 1-4, with 4 indicating stronger capability.

Identification[3] of key assets, services and third parties

3.7. Most firms report that they understand what information they have (their information assets) and their critical business functions. However, they described challenges in maintaining this picture. They had similar issues in maintaining a view of their third parties[4] and managing end-of-life assets[5]. Assets can only be protected if they are identified, and their sensitivity and criticality to a firm's business understood. Keeping this view up-to-date is necessary to quickly assess the scale of any cyber-attack and respond appropriately.

3.8. While firms have established processes to identify their information assets, they are unable to consistently and regularly review and update them as needed. Seventy nine percent of firms said they knew what their critical assets were. However, only 56% of firms regard themselves as able to measure the effectiveness of their controls in this area.

3.9. Most firms reported that they regularly review their hardware and software assets to determine those nearing end-of-life. However, many do not maintain a continuous view and / or rely on ad hoc or manual processes. When reviews do take place, nearly half of firms do not upgrade or remove end-of-life assets within a reasonable timeframe. Nor did they describe any increased risk management practices that are carried out until the assets are replaced.

3.10. There is a significant risk that vulnerabilities of unsupported assets are not identified and fixed in a timely way. This is a regular route for attackers. We are concerned that firms are not addressing the more obvious risks presented to their business and customers by their technology estate.

---

[3] The FSB Cyber Lexicon defines the Identification function as 'developing the organisational understanding to manage cyber risk to assets and capabilities'. The FSB Cyber Lexicon defines Asset as 'something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation'

[4] In this context, we mean any arrangement between a firm and a service provider by which that service provider performs a process, service or activity which would otherwise be undertaken by the firm itself.

[5] All software/hardware has a date at which the vendor ceases support. Support includes updates to protect against previously unknown attacks which will no longer be provided for out of support hardware/software

Information sharing

3.11. Survey responses suggest that larger firms, particularly in the retail and wholesale banking sectors, are more willing to share information through established mechanisms than those in other sectors. These firms are more likely to be members of one or more information-sharing forums or platforms, including the NCSC's Cyber Information-Sharing Platform (CiSP).

3.12. However, even within these sectors, some firms said that they choose not to share relevant information or had an ad hoc approach to information sharing or gathering. This may undermine firms' ability to provide or seek help in the event of a cyber-attack affecting the wider sector. Reputational damage or providing an incentive for other attackers to focus on them if the information they had shared were to be leaked, were given as reasons for not sharing information.

3.13. Many firms reported that they 'pull' information, subscribing to networks and information-sharing platforms to monitor for events or incidents but are not routinely contributing to them. These were typically the smaller firms, who (if giving an explanation) said that they do not think they have relevant information to share.

3.14. This lack of consistency suggests that there could be more effective collaboration across the industry. We encourage all firms to take a more open approach to information sharing with their peers, and to consider whether the information they hold would provide valuable context to others in their sector or the wider industry.

High-risk staff and a security culture

3.15. Ninety percent of firms confirmed that they operate a cyber awareness programme. This is positive but, as it is a fundamental element of security, we are disappointed that not all firms operate one.

3.16. Firms described difficulty identifying and managing their high-risk staff, such as those who deal with critical and sensitive data (for example, executives and their assistants, HR and finance personnel, as well as those with privileged system access). **Even where firms did identify staff in high-risk roles, only 47% of firms said that they provided additional cyber training for them**. Training was described as ad hoc rather than regular or ongoing. This means staff may not be properly educated about, or prepared for, the increased risks that they will encounter in their roles.

3.17. Given the prevalence of social engineering and phishing as a means of cyber-attack, often targeting these roles, this presents a significant weakness. In many cases this risk is compounded by a simultaneous lack of monitoring of staff activity, so firms are unlikely to detect anomalies in staff behaviour and subsequent activity.

3.18. Many firms recognise there are threats posed by 'insiders' and consider these to be some of their most significant cyber-risks. However, in our broader supervisory work, we have seen only limited evidence of firms proactively seeking to 'connect the dots' between cyber and other conduct issues which may be enabled through cyber channels (eg market abuse and financial crime). The ability of any employee within the firm's perimeter to either intentionally or negligently give rise to cyber-attacks emphasises the importance of embedding a 'security culture' which runs through all aspects of an organisation. An effective technical control environment alone may not reap the best results if it is not accompanied by positive, methodical steps to increase staff awareness.

Detecting Attacks

3.19. Only the largest firms report that they have automated systems to spot potential cyber-attacks and support their subsequent response. Smaller firms are mainly reliant on manual processes, or have no processes at all. This could delay their ability to respond to fast-moving incidents such as those seen with WannaCry and NotPetya.

3.20. Across the cyber survey we saw inconsistent capabilities. This should be a focus for firms because weaknesses in one area, for example detecting attacks or monitoring staff activity, are likely to undermine stronger capabilities in other areas. Cyber resilience requires a focus on all these areas simultaneously.

Change management

3.21. Change management is a well-established technology discipline. So, we would expect most firms across all sectors to have assessed themselves as mature in this area. However, there is a disconnect between firms' self-assessed strength in change management and our analysis of incidents reported to the FCA. This indicates that poor change management caused 20% of incidents reported to the FCA between October 2017 and September 2018.

3.22. We recognise that firms need to make regular changes – of varying size and complexity – to their technology estates, and that from time to time things will go wrong. This is reflected in our recent joint Operational Resilience discussion paper (DP).

3.23. However, the responses indicate that some of the concepts set out in the DP (such as the identification of important business services and the need to focus on recovery plans and customer communications) are not yet part of all firms' thinking. We will be doing further work over the coming year to assess the sorts of changes, and poor change management practices, which give rise to the incidents reported us.

Managing third parties

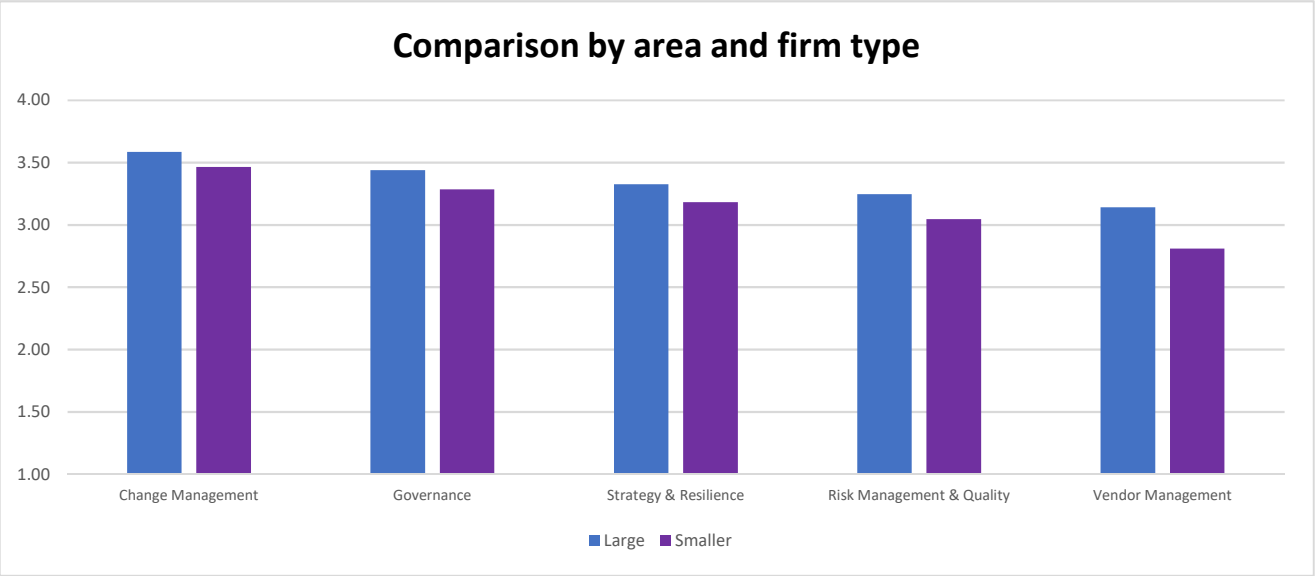
3.24. Eighty percent of firms reported that they maintain a register of third parties. However, half of firms said that they do not maintain a **comprehensive** list of all third parties with whom they do business and which access their systems and data. Without this understanding, it will be difficult for firms to appropriately assess the criticality of third parties, and the subsequent risk to services they provide.

3.25. We recognise the scale of this challenge, particularly at the largest firms. However, the adoption of a risk-based approach to assessing the criticality of each third party and the potential impact caused in an adverse situation is fundamental to resilience.

3.26. Nearly all firms described discussing cyber risk with their third parties. However, only 66% of large firms and 59% of smaller firms understood their third parties' response and recovery plans. These figures drop to 22% and 19% (respectively) when it comes to explicitly including third parties in their own testing plans.

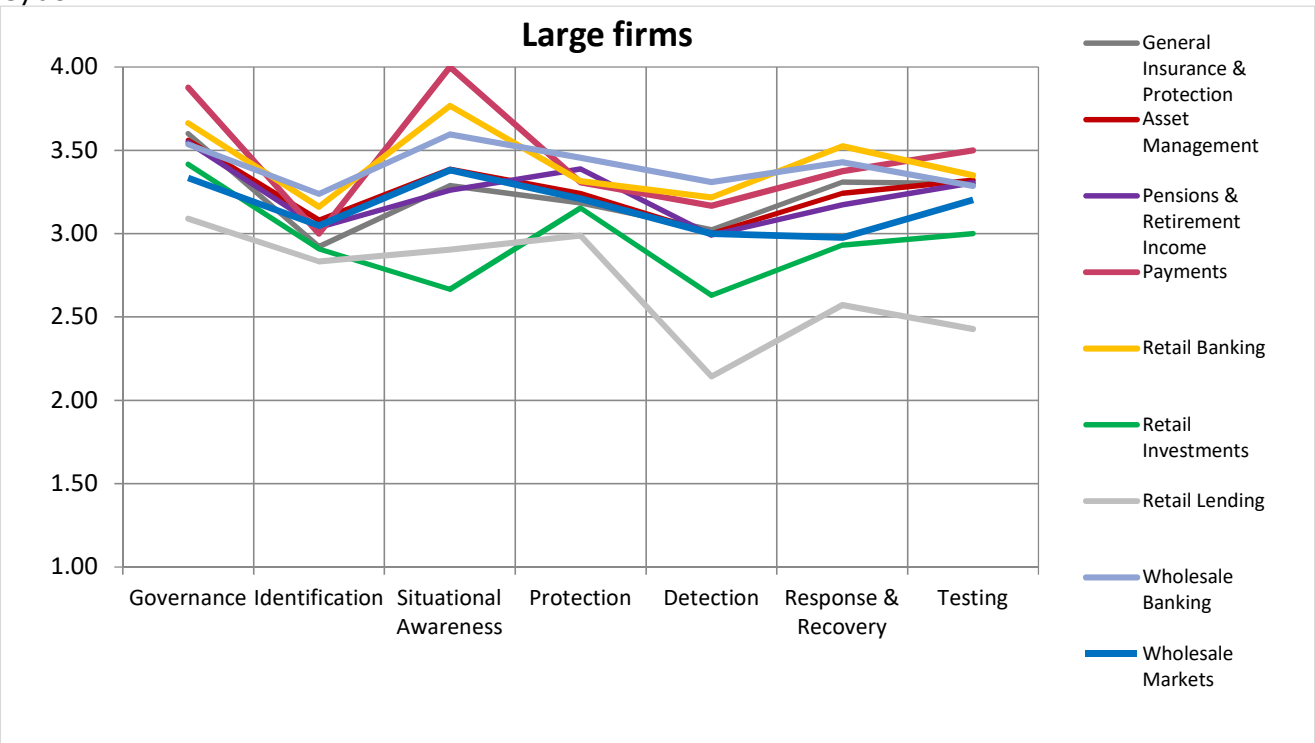
3.27. We are disappointed with these responses given the wide understanding of the risks third parties pose to firms' operational resilience, and the number of incidents involving third parties. For example, firms in the pensions and retirement income

sector assessed themselves as having mature supplier and vendor management capabilities. However, recent operational incidents, including issues with suppliers and subsequent customer service, suggest that the challenges in this area are not yet effectively managed.

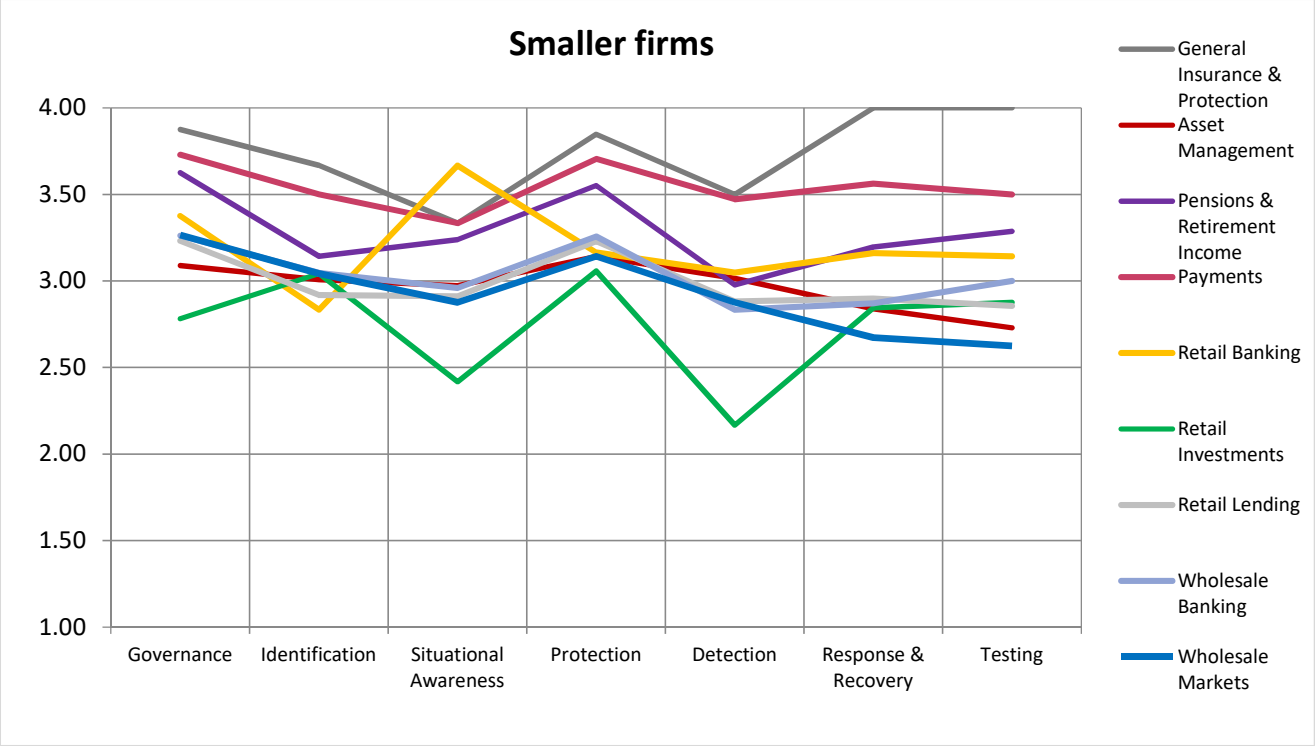


3.28. Across the cyber survey results there was less variance between the self-assessments of larger firms than those of smaller ones. The sectors where firms assessed themselves as less mature are those made up of larger numbers of smaller firms. This indicates that these firms require a better understanding of our expectations and sources of information. The National Cyber Security Centre (NCSC) has issued guidance that may be of help to smaller firms.

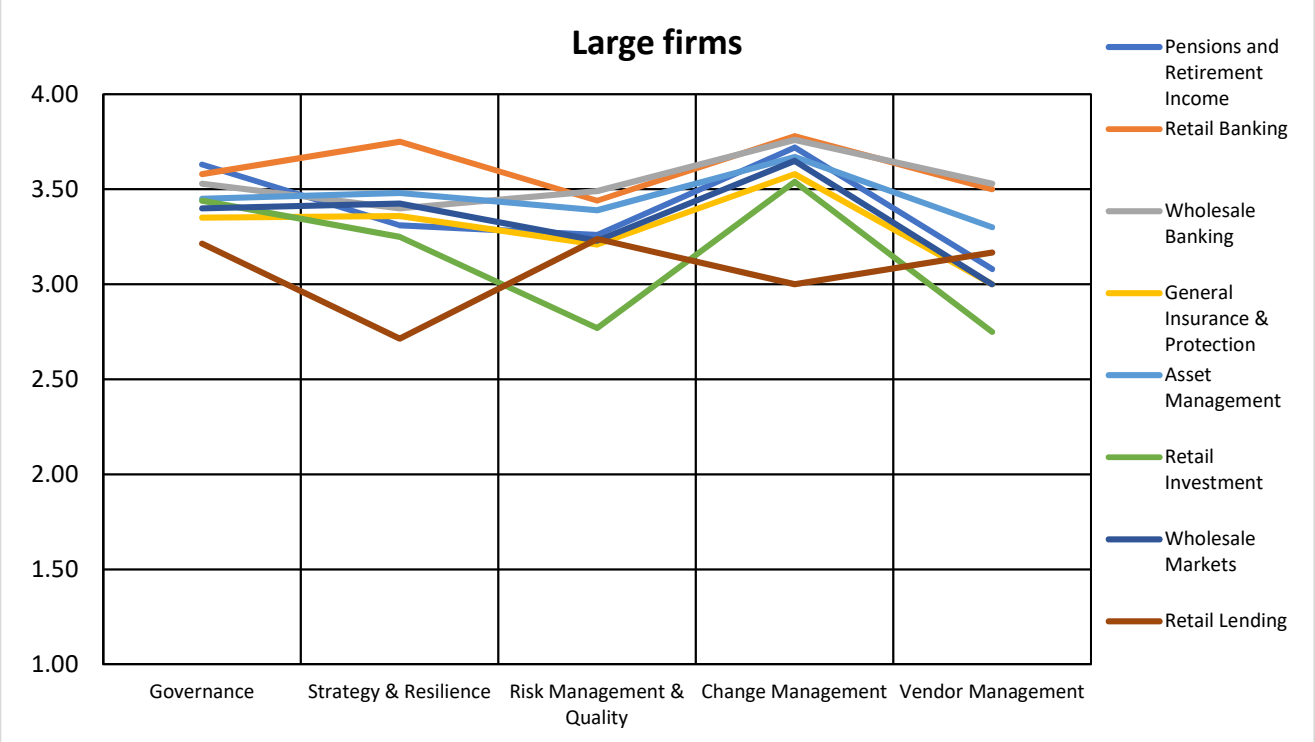
Cyber:

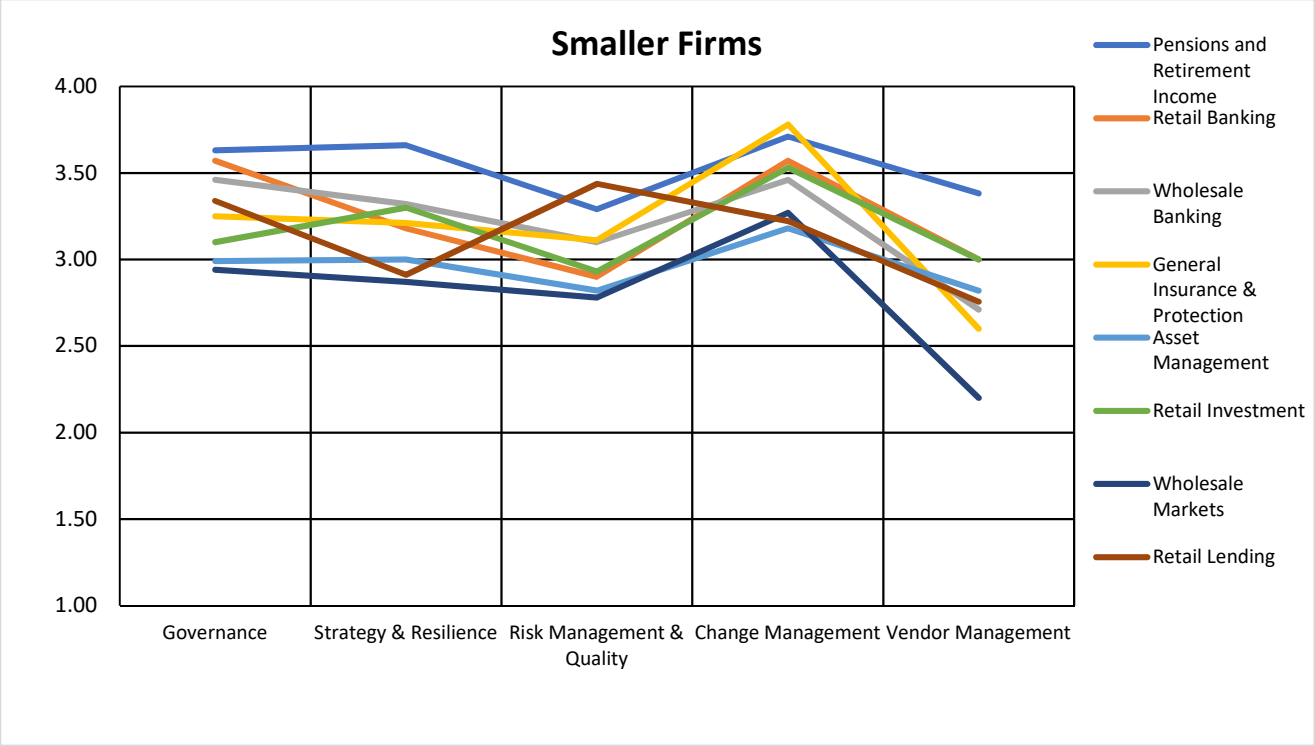


Note: For each question firms assessed themselves on a range from 1-4, with 4 indicating stronger capability.


Smaller firms
4.00
3.50
3.00
2.50
2.00
1.50
1.00
Governance
Identification
Situational Awareness
Protection
Detection
Response & Recovery
Testing
General Insurance & Protection
Asset Management
Pensions & Retirement Income
Payments
Retail Banking
Retail Investments
Retail Lending
Wholesale Banking
Wholesale Markets

Technology:


Large firms
4.00
3.50
3.00
2.50
2.00
1.50
1.00
Governance
Strategy & Resilience
Risk Management & Quality
Change Management
Vendor Management
Pensions and Retirement Income
Retail Banking
Wholesale Banking
General Insurance & Protection
Asset Management
Retail Investment
Wholesale Markets
Retail Lending



4. Next steps

4.1. All firms should consider the findings and feedback in this report and its relevance to their business. Firms which have received individual feedback on their survey responses should consider this report as additional context.

4.2. The information gathered through this exercise supports our ongoing assessment of firms' resilience, and helps to identify examples of good or poor practice. Key areas of focus, that we have identified, such as third party management and change management, will be considered in our supervisory plans for 2019.

Annex 1

5 Over 2017 and 2018, we surveyed 296 firms across:

- wholesale financial markets
- wholesale banking
- asset management
- retail lending
- pensions and retirement income
- retail investments
- retail banking
- general insurance and protection
- non-bank payment services

5.1 All firms were asked to complete a self-assessment survey; with questions to assess both technology and cyber resilience. The surveys consisted of multiple choice statements from which firms self-selected the response that most closely aligned with their current approach; firms could add free-form text to further clarify or support their responses.

5.2 296 firms were covered by the technology resilience survey and 256 by the cyber resilience survey. A smaller number of firms were covered by the cyber survey as they had been assessed in previous supervisory work.

5.3 The technology and cyber parts of the survey are different in form and purpose. The technology survey had not been used before and was intended as a discovery assessment tool, designed to identify areas where we may focus future attention. A form of the cyber survey has been used by the UK regulatory authorities since 2013. This survey was more detailed, allowing us to use it to identify more specific issues; questions were developed in line with several commonly used frameworks[6].

5.4 The cyber resilience self-assessment survey contained 46 questions across seven domains aligned to the National Institute of Standards and Technology (NIST) framework and National Cyber Security Centre advice[7].

5.5 We asked firms a smaller and higher-level set of questions in our technology resilience survey. We asked 28 questions over 5 technology areas:

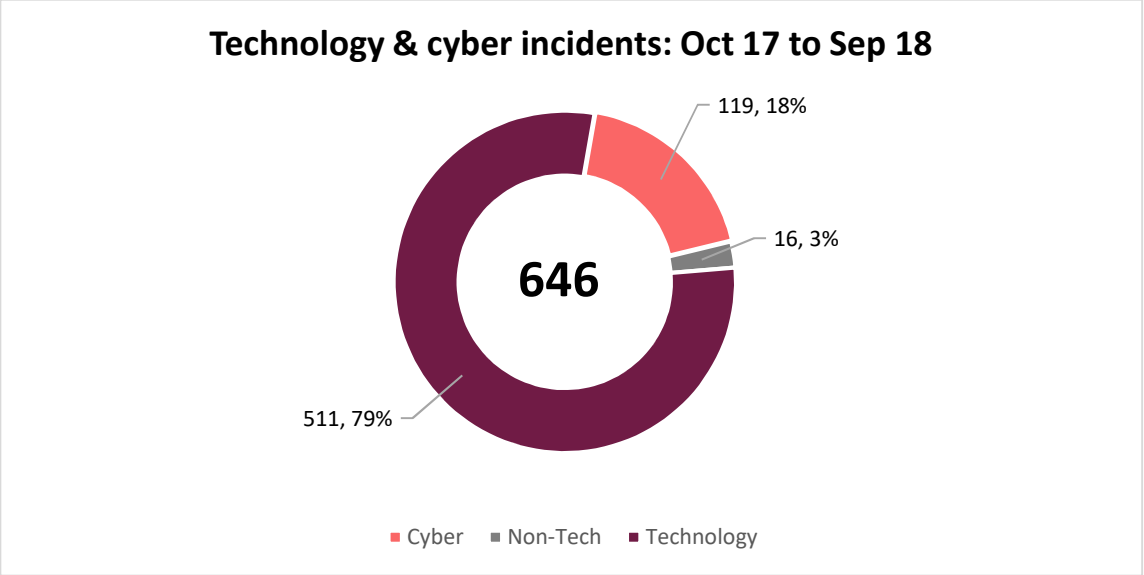
- Strategy and Resilience
- Governance
- Risk Management and Quality
- Change Management
- Supplier and Vendor Management

5.6 Our analysis of firms' self-assessments also included comparison between the findings of the surveys and the data we hold on incidents reported by firms to the FCA. As mentioned earlier in the report, we expect firms to report material incidents to us under Principle 11. For those firms subject to the second payment services directive reporting should be in line with the guidance in that directive.

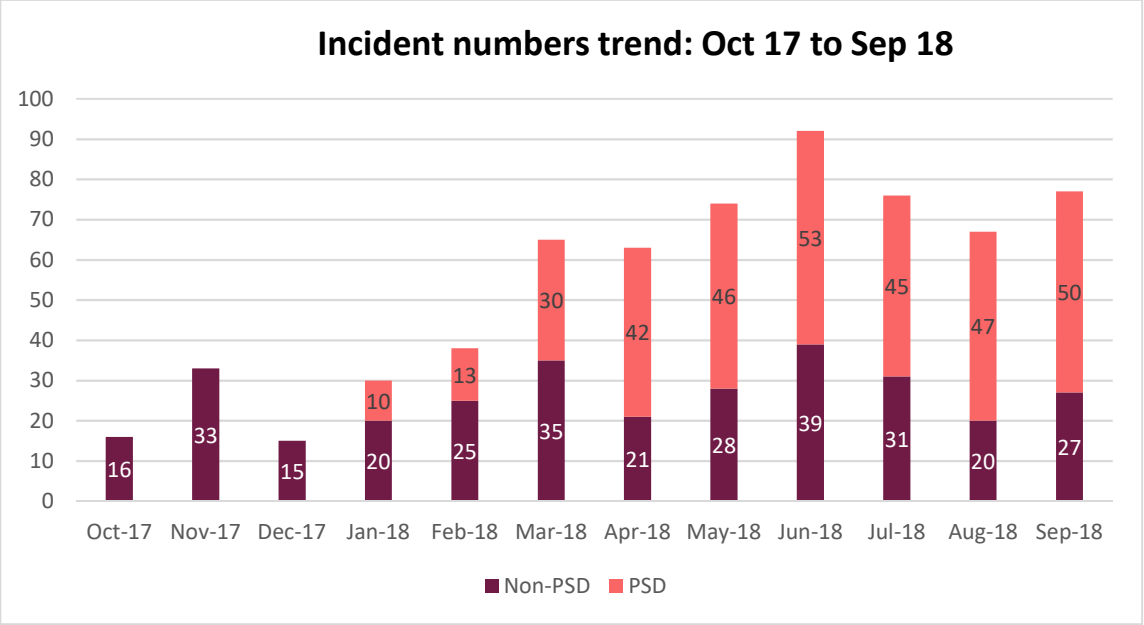
[6] CPNI PerSec, NIST, IOSCO, SANS CSC, FFIEC, NCSC Cyber Essentials, ISF SOGP and ISO/IEC27001:2013

[7] NIST covers: Governance, Identification, Situational awareness, Protection, Detection, Response and Recovery, Testing

Incident data analysis for the survey period – October 2017 – September 2018



Note: Non-technology events include incidents such as flooding.



Note: New reporting requirements came into force in January 2018 for firms subject to the second payment services directive which has resulted in an increase in the number of incidents reported to us.