FINANCIAL CONDUCT AUTHORITY

Cyber security - industry insights

March 2019

Contents

How to navigate this document

returns you to the contents list

takes you to the previous page

takes you to the next page

prints document

1 Introduction

Sharing insights on cyber

1.1 Cyber is complex and unpredictable, and sharing information is vital to successful cyber defence and resilience. Since 2017, the FCA has brought together over 175 firms across different financial sectors to share information and ideas from their cyber experiences. We run these cyber coordination groups (CCGs) with industry, to help promote understanding and awareness of innovative cyber practices.

1.2 The principal objective of the groups is to aid the improvement of cyber security practices amongst members of the CCGs and their sectors. We hope the practices and experience of the groups will benefit other firms, so we are publishing these insights to help those firms not already involved.

Cyber coordination groups – who they represent

1.3 The CCGs are sector-specific, and we invited firms to give a representative sample of the sector, based on cyber maturity. In 2017, the cyber coordination groups represented the following sectors: fund management, investment management, insurance, retail banking, and retail investments and lending. An independent association, the Investment Banking Information Security Special Interest Group (IBSIG) has similar objectives. Although it is not co-chaired by the FCA, we have a standing invite.

1.4 In 2019, we will be creating 2 new groups to increase the representation of trading venues and benchmark administrators, and brokers and principal trading firms.

Sharing themes to inform the wider industry

1.5 Since we created the CCGs, we have been actively investigating ways to share the outcomes and key themes with a much wider financial sector audience. As our 2017/2018 cross-sector survey showed, smaller firms assessed themselves as having generally less cyber capability than larger firms. They also showed a higher degree of variance in their self-assessments. This indicates a need for a better understanding amongst wider industry of insights and practices.

1.6 Over the last 12 months, the groups have been discussing and sharing innovative practices in the following discussion areas: Governance, Identification, Protection, Detection, Situational Awareness, Response and Recovery, and Testing. We have collated the examples shared by firms and set out those we consider to be beneficial for a wider audience under each of these themes. These may particularly help small and medium-sized enterprises.

1.7 This document should not be considered FCA guidance. It does not set out what our expectations are in terms of what systems and controls firms should have in place to comply with our regulatory requirements. Each of the examples here have been shared by one or more firms within the CCGs, and many support existing guidance from the National Cyber Security Centre (NCSC).

Practices and experiences

2 Put good governance in place

2.1 Governance enables an organisation to control, direct and communicate their cyber- security risk-management activities. Governing how risks to technology systems are managed should be no different to the way organisations govern other business activities. The CCG members agree there is no 'one size fits all' approach to governance. Organisations should establish the security risk-management roles and decision-making processes that work for them. This supports the NCSC approach to security governance.

2.2 Firms shared the following practices and insights for governing cyber. They are aligned to business objectives and considered as part of the risk-management framework in their businesses.

A top-down approach

- **Put cyber risk on the executive agenda.** Use an enterprise risk management approach to articulate and share cyber risk related to business operations, customers and reputation. This will help executives place cyber risk within the appropriate context, and consider it when running their businesses.

- **Educate the executives.** Run workshops with executives to increase cyber knowledge. Use case studies and incidents reported in the media to highlight potential risks and help executives link these risks to their business.

- **Present high-quality management information in useful formats.** Present a simple dashboard to executives that illustrates what is good, what needs improvement and what is inadequate. The management information helps articulate cyber risk in terms of risk that people already understand, such as financial losses or brand damage. See the NCSC on this.

Make it simple

- **Adopt plain language to articulate cyber.** Use language that staff and executives understand and relates to their day-to-day business activities.

- **Recruit champions.** Appoint influential members of staff who understand and are interested in cyber to act as a bridge between cyber and the business. They also work the other way, through providing an understanding of the business that technology and security functions cannot always see.

Think bigger picture

- **Understand who could target your business, why, and how.** Understand what data is valuable to which malicious actors. Creating profiles for groups such as hostile nation states, organised criminals, activists, and amateur hackers helps understand their goals and capabilities.

- **Ensure there is a link between risk and controls.** Controls exist to mitigate risk. Create metrics and indicators for critical controls to understand whether they are functioning effectively. Without understanding the effectiveness of controls, it is difficult to know if risks are being managed.

- **Use existing standards.** Standards provide valuable frameworks devised from good practice; consider the NIST Cybersecurity Framework, ISO27001/2, SANS CIS, NCSC's 10 Steps to Cyber Security or NCSC's NIS Directive Cyber Assessment Framework, Cyber Essentials, etc.

3 Identify what you need to protect

3.1 The complexity of organisations and the pace of change makes it difficult to keep track of your information and systems, and how they are linked and managed. The identify domain highlights the importance of understanding what it is you are trying to protect and how entities are linked. Without this it is not possible to take a risk-based approach within all other domains.

3.2 Firms shared the following insights and practices:

Consider what you already know

- **Use guidance.** Use the guidance already available on GDPR Security Outcomes to create and maintain a list of information assets. This includes how business services and processes use them.

- **One view is the wrong view.** Consider assets from multiple perspectives and draw in data from many sources. This will help build and maintain a complete picture of the assets you are trying to protect. It might include combining the output of information asset management, system asset management and business services. You should also use change management records, vulnerability scans, anti-virus management consoles and other sources.

Understand who you work with

- **Where do you spend your money?** Ask the Finance department for a complete list of suppliers.

- **Functioning in an eco-system.** Understand the connectivity between and dependency on partners. Adopting the view that you only need to be concerned with suppliers limits the ability to think wider about third party risk.

Have a whole business understanding

- **Business continuity.** Use information captured from Business Impact Analysis to build a picture of which business services need to be protected and how critical they are.

- **Know your business.** Stay plugged into new business initiatives so that you can judge how cyber will need to adapt to the business in the future.

4 Protect your assets appropriately

4.1 Tackling external threats requires effective cyber security policies, standards, procedures and controls. These will protect the confidentiality, integrity and availability of your business services, while limiting and containing the impact of a potential cyber incident.

4.2 Firms shared the following insights and practices:

Invest in training

- **Continual improvement.** One-off cyber security and awareness exercises do not guarantee security. Think long term and design a user education and awareness programme that constantly weaves cyber security into the culture and behaviours of your organisation.

- **Be targeted.** Target training the same way a cyber criminal might target specific individuals, groups of users or a department, such as those with access to critical systems. Align training with your employees' roles, responsibility, duties and access to data.

Manage your third-party suppliers

- **Remember that you cannot transfer the responsibility.** Ensure that cyber security and legal language are added to any contract with the right to audit. Review old contracts to ensure that you know your position with third parties.

Use encryption

- **Too little or too much.** Apply encryption controls proportionately. Not all data requires every control to be applied. You should apply risk management principles to determine the impact of data being exposed, based on its classification policy.

- **Only as strong as your weakest link.** Define and monitor the policy and procedural controls protecting unauthorised access to your cryptographic keys.

Be aware of your vulnerabilities

- **Know your weaknesses.** Identifying vulnerabilities, weaknesses or flaws that might be exploited is a continuous exercise. Any holes in your cyber security could allow malicious intruders to gain a foothold in your organisation.

- **Know your digital footprint.** Cloud and mobile technologies have extended the traditional on-premise ways of working and delivering resilient business services. You may find your digital footprint is larger than expected.

- **Prioritise and fix.** It is not uncommon to discover huge quantities of vulnerabilities to assess. Knowing the criticality of assets through a Business Impact Analysis helps prioritise which to fix first, and will enable better reporting of your improvements.

- **Not all vulnerabilities can be fixed.** Some legacy systems or software cannot be upgraded or modified. In this case you can apply and test alternative compensating controls to reduce the risk.

- **No need to re-invent the wheel.** Use existing security configuration standards such as CIS Benchmarks or NCSC secure configuration guidance as a starting point. Once the standards have been formalised they are built into the security requirements when designing, modifying or upgrading a business service.

Make cyber security part of your change management process

- **Security by design.** Include your cyber security team as part of the change management and assurance process. This helps incorporate cyber resilience at the earliest stage of design, development and system acquisition. It means they will be there throughout the system development lifecycle and into your change-management processes.

5 Use good detection systems

5.1 Firms must be able to detect actual or attempted attacks on systems and business services. Thorough and effective system monitoring is essential to detection and helps to ensure that systems are being used in line with organisational policies.

5.2 Firms shared the following insights and practices:

Tackle the insider threat

- **Who's who.** Tie specific users to specific accounts through your identity and access management processes. This gives you a solid basis for ensuring individuals have appropriate access rights, and correctly attributing system misuse.
- **Know your privileges.** Identify users with privileged access to critical systems, and review this on a regular basis. Heighten monitoring on these systems and consider using Data Loss Prevention tools.
- **Monitor behaviour.** Use network behaviour monitors and user behaviour analysis to identify deviations from the expected patterns of activity. Pay particular attention to users with access to critical systems.

Establish an effective monitoring regime

- **Use the right information for you.** Choose which logs to collect based on your unique circumstances, and generate alerts that are relevant. Ensure these allow you to see external network communication, cloud services and third parties to detect Indicators of Compromise.
- **Tamper proof.** Prevent cyber criminals removing traces of their actions by segmenting, monitoring, alerting and applying strong access controls to audit database logs.
- **Validate.** Review and assure your log sources are working as intended. Configure alerts when systems stop forwarding logs. Being unable to restore your archived logs during an incident will make it harder to recover. Check that your archived logs can be securely restored and are searchable.
- **Synchronisation.** Use a resilient authoritative time source across all the organisation's systems.

6 Be aware of emerging threats and issues

6.1 You need to be alert to emerging threats and issues to make informed cyber resilience decisions. This intelligence may come from a variety of internal and external sources, which highlights the importance of sharing intelligence when possible.

6.2 Firms shared the following insights and practices:

- **Participate in forums.** Incorporate the sharing of information and intelligence in recognised information-sharing forums into your incident response plan. Pooling data and insights means you and your peers are more likely to benefit from these forums.
- **Feed into planning.** Use plausible scenarios or examples from the media to continuously improve and refine how information is shared and communicated to internal and external stakeholders.
- **Learn from others.** Use the events that have affected others and assess the impact against your own firm and defences. Ask yourself if your firm would have been protected against that incident? Or would that event even affect your firm? You can learn lessons from both internal and external incidents.

7 Be ready to respond and recover

7.1 Incidents will occur. The ability to respond and recover from them should be a key part of a business's risk management and operational resilience planning. Resuming critical business services rapidly and with accurate data requires continuity planning and testing of plausible cyber-attack scenarios. Exercising people, processes and technology is a key aspect in preparing response and recovery planning.

7.2 Firms shared the following insights and practices:

Create scenario-led exercises

- **Test plausible scenarios.** Plan on the assumption that the inevitable will happen, and test plausible scenarios tailored to your business. Identify your critical services, people, processes and third parties that underpin these services to assess the impact on your business.
- **Make recovery decisions before an incident happens.** Define your business tolerance for the recovery of individual systems and data using Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) to minimise the need to make pressurised recovery decisions during an incident. Review these objectives regularly to ensure they are right for your business.
- **Lessons learnt.** Allocate enough time and resources for reviewing information captured during a cyber incident. You can use this to improve your response and recovery controls.
- **Inception to reporting.** Evaluate and exercise your cyber capabilities and business processes by creating and executing plausible threat-driven playbooks. These should focus on assessing the effects on your critical business services.

Investigate all incidents

7.3 **Know the basics.** The ability to conduct basic investigations is key. Train your team with the necessary skills or bring in specialist consultants or third parties. Simulate an incident investigation process end-to-end to familiarise them with the process.

Know how to communicate

7.4 **Make it work internally.** Establishing and testing internal communication channels with key decision makers will make key decisions faster and simpler in a crisis. It will also ensure people know who is accountable for decisions.

7.5 **And externally.** Run stakeholder communication practise by creating a multi-channel incident response plan while maintaining a consistent message.

8 Test and refine your defences

8.1 Testing the cyber defences of your whole organisation ensures you understand the effectiveness of controls across people, process and technology. A strong testing regime helps develop a culture for continuous improvement as issues are discovered and fixed.

8.2 Firms shared the following insights and practices:

Create a comprehensive framework

- **Continual improvement.** Review exceptions, non-conformities and perform root-cause analysis of incidents and near-misses to help challenge the effectiveness of policies, standards and procedures.
- **Emulate the threat.** Use more than one method to identify and assess your security vulnerabilities. Considering a variety of proactive methods may provide greater clarity (for example, penetration testing, phishing simulations, vulnerability scanning, red/purple teaming).
- **Testing approach.** Consider the views of your users and security operations centre when deciding what testing approach to take.
- **No assumptions.** Do not work on the assumption that controls are operating effectively. Use information about your controls and their objectives to create and run tests to understand if the controls need to be improved or replaced.

Invest on testing and training staff

- **Make reporting easy.** Implement easy ways for staff to report phishing (such as a button on your email toolbar) and procedures that deal with reported phishing emails.
- **Adopt password testing.** Test employees' passwords across exposed credential dumps along with commonly used credentials.
- **Continuous development.** After identifying areas of weakness and providing staff training sessions, reassess these areas to test the effectiveness of the program.

9 Next steps

9.1 We encourage all firms to consider whether these insights may be useful to them in considering their own cyber resilience. The insights are also shared with the other financial authorities who attend CCG meetings, including the Bank of England and the NCSC. The insights provide a valuable input to help shape NCSC advice and guidance.

9.2 Sharing information is vitally important to increasing levels of cyber resilience in the financial industry. Over the next 12 months we will continue to look for ways to communicate insights and innovative practices shared within the CCGs with the wider financial community.

Pub ref: 005905

12 Endeavour Square London E20 1JN
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk