Image: Christoph Scholz

Report

Cyber Resilience Leaders' Summit

Monday 8 – Tuesday 9 October 2018 | WP1621

Wilton Park

Report

Cyber Resilience Leaders' Summit

Monday 8 – Tuesday 9 October 2018 | WP1621

In association with UK Finance

The threat assessment

In 2018 the UK financial services sector is on the front line of the rising challenge of cyber-crime. Every day cybercriminals are probing its defences, seeking ways to access the data of customers or their assets. While cyberattacks are routinely rebuffed, when they succeed the costs in reputation and customer confidence are high.

The financial sector's changing digital profile is driving a revolution in banking and financial services, but it is also at the heart of what makes it vulnerable. The digital storage of customer data and assets in centralised storage systems, often legacies of mergers and acquisitions, represents a rich target for cybercriminals. The deployment of financial data across payments systems and platforms and billions of connected devices creates an expanding attack surface and many points of vulnerability, often beyond the direct control of banks themselves, even when it is bank data that is being exposed to risk. The demands of security discipline and prudence on tens of millions of customer-users is an inevitable source of potential vulnerability.

The attackers themselves are also evolving. At its elite level, cybercrime is a complex and sophisticated business model, and often a low volume, high value one. Its modern practitioners are unhurried and deliberative, willing to monitor targets for points of weakness, gather data and lie in wait while they judge the right time to exploit vulnerabilities. The line between nation-state and criminal attacks has blurred, as has the line between conventional organised crime and cyber-crime. The same individuals and groups will often be involved in all three. Attackers move quickly, and their actions are often hard to attribute.

What does a cyber resilient UK financial services sector look like?

1. Against this rapidly changing threat landscape, it is necessary to ask: what does a resilient UK financial services sector look like? For a sector already heavily focused on adapting to major changes in regulatory frameworks such as the EU Markets in Financial Instruments or the Payments Services Directive II, or implementing the far-reaching changes brought about by the General Data Protection Regulation, resilience to cyber attack needs to be integrated into these adaptations.

2. Debate and discussion at Wilton Park identified four key channels for the industry to focus on in the months ahead. Each contains an important agenda of action for individual firms and for collaboration within the sector, and with its regulators, policymakers and other economic actors. The core challenges were identified as:

    - A new collective discipline of cyber resilience planning;
    - Better intelligence sharing;
    - A deeper cyber risk culture in firms – from practitioners to Boards;
    - A new dialogue with the public.

A new collective discipline of cyber resilience planning

3. Cybersecurity demands a new set of protocols and practices for financial services firms. But many of these can draw on, and learn from, existing risk management practices.

4. First, the UK financial services sector needs to continue to develop a comprehensive picture of its own vulnerabilities to cyber-attacks and continue to develop the professional discipline of reaction and response to attacks. At the firm level, this means mapping the services exposed to cyber-attack. This can mean focusing not only on points of potential weakness in IT systems, but in the scale of the knock-on effects of disruption across service lines, and ultimately for market stability.

5. In parallel, firms need to develop a clear sense of their tolerance for disruption from the perspective of service users. A firm's definition of recovery from a cyber attack needs to reflect the service continuity expectations of customers, as well as the operational preferences of the firm itself. Defining customer harm is not simple in a market in which customer expectations of service availability are typically very high, but where a balance needs to be struck between harm and inconvenience for resilience purposes.

6. Second, this model of risk and exposure needs to extend beyond the financial sector itself into its supply chain and into service providers such as telecommunications and cloud computing suppliers. It also needs to reflect the ways in which sensitive banking data can travel across the online economy with customers and other commercial actors in a way that leaves banks exposed to costs and reputational risk, even when the data is no longer being held within their own secure environments.

7. Financial service firms have an important role to play in pushing out best practice to customers and the firms in the financial ecosystem such as merchants on payments platforms who are responsible for the data of their customers. Groups like the UK Cross Market Operational Resilience Group (CMORG) are an important platform for driving this sort of dialogue and collective action.

8. Third, the industry needs to accelerate and deepen its use of exercises to stress test its developing protocols for cyber resilience and recovery from cyber-attack. This should include both firm-level testing and large-scale exercises designed to test issues of sectoral and systemic resilience and cooperation. This is not something that should be left to regulators, although they may be involved. The outcomes from such exercises should be systematically fed back into cyber resilience playbooks.

9. In this respect, banks already have the developing discipline of recovery and resolution plan testing to draw on. Transferable approaches from this area include the basic discipline of regular testing; an open and iterative approach to feeding results back into evolving cyber-resilience plans; and a recognition that there is an important public-facing role for such exercises in signalling a level of preparedness and resilience. Embedding regular stress testing can help executives move past debating the probabilities of attack or breach and focus them instead on the necessary preparations for major incidents, even if these remain low probability events.

Better intelligence sharing

10. The effective sharing of intelligence and data is an integral part of effective collective action against cybercrime. Tracking activity across firms can be an important way of identifying conduct patterns and attributing illegal activity. Issuing warnings of suspicious practice and proactively flagging suspected risks can contribute to faster adaptation to potential risks and anticipation of possible attacks. Ensuring that the data shared is high quality and actionable is as important as establishing the mechanisms of exchange.

11. In this area, practice in the UK is improving, but more could be done. Intelligence sharing with the authorities can be (or feel to firms) one way: firms escalate information on suspicious or harmful activity to law enforcement but can receive limited feedback on the value or subsequent use of the information they share. Contact also remains overwhelmingly bilateral, with firms often unaware of the ways in which their peers are sharing information with law enforcement, even on linked activity.

12. Intelligence-sharing needs a clear framework that covers both questions of trust and legal liability. In the former case, some firms remain reluctant to share information with authorities out of concern that it may be deployed against them for regulatory purposes. More acutely, the sharing of customer data can only take place with the most robust of legal protections. Models for doing this that have developed in the areas of anti-money laundering are potentially transferable to this area. An important immediate aim should be to establish a set of industry protocols for sharing intelligence and data with the National Cyber Security Centre. The evolving protocols for intelligence sharing that have developed around the Joint Money Laundering Intelligence Taskforce system have lessons for the sector in this area.

13. It is also important to consider the ease with which intelligence can be understood and disseminated across financial services firms. The spectrum of sophistication across the 50000+ UK regulated financial services firms in this area is inevitably very wide, ranging from large specialist departments to a single individual. Bringing smaller and less resourced firms effectively into an ecosystem of cyber-resilience cooperation means ensuring that they are fully aware of – and equipped to – manage the upward escalation of intelligence, and to understand how to contextualise, interpret and act on intelligence being disseminated to them.

A deeper cyber risk culture in firms – from practitioners to Boards

14. Cybersecurity is not just about technological strategies for blocking the penetration of cyber defences. It is about building an entire culture of risk management that is fully integrated into the basic view of a firm's resilience.

15. Genuinely cyber-resilient financial service firms are ones that can build bridges of communication between practitioners and executives and business functions. While the skillsets of managing modern information technology are absolutely critical to risk management, so are the capacities to socialise technology risks, to escalate issues effectively and clearly, and to manage the intense firefighting and communication protocols that are an integral part of any effective response to a breach.

16. Boards and senior managers are increasingly accountable for processes and protocols on which their technical competence is simply not adequate. While this can in part be addressed by promoting technical specialists into these positions and by investing in raising the competence of executives to the point where they can make meaningfully informed judgements about risk, metrics and courses of action, this is not enough. The process also requires specialists that can distil issues and choices to a point where an intelligent and informed dialogue with executives can take place.

17. There is also a general need to focus on the general pool of cybersecurity skills in the UK, which is currently too limited for the evolving demands of the financial services sector. The sector needs to take a collective view of building and encouraging a pipeline of technical specialists and cyber breach management experts. This can be encouraged by engaging with training bodies, effective apprenticeships, mentoring and secondments and an intensive approach to training that accepts that, although cyber-security professionals may display a high preference for mobility, the industry benefits from a generally high level of skills and a deep pool of expertise. As noted above, this view of the necessary skillsets for a cyber-resilient sector needs to extend well beyond a core set of IT professionals into legal, communication and crisis management skills.

A new dialogue with the public

18. Financial services customers and the general public need to be part of a wider approach to cyber resilience in the UK. This requires a new open and frank dialogue with them. The customers of financial service firms represent a crucial line of defence for cybersecurity in the way they manage their own data and understand how to identify threats to their data security or privacy. But communication with the public needs to go further than simply helping instil a high level of prudence and risk-awareness in their personal online conduct.

19. As it has in the area of counter-terrorism and economic crime, effective communication by law enforcement and the public sector has an important role to play in conditioning a wider public understanding of the scale of the threat, the scale of the unwanted activity that is being detected, deflected and prosecuted, but – to some extent – the inevitability that some breaches will nevertheless occur. It is also an important way to calibrate expectations of what constitutes unacceptable disruption in the face of cyberattacks in an era of 24/7.

20. As in other areas, in the area of communication with the public on cybersecurity, attempts by individual firms to exploit the weaknesses of peers in public communication for competitive advantage risk being seriously counterproductive and short-sighted, as it erodes public confidence and a culture of security collaboration. Effective communication will be best led by the public sector. Supported by efforts from the financial sector which also need to be supported by responses with online retailers and service providers when they are coordinating the breaches of consumer data on their networks.

A new phase of collective action

21. A fifth important theme at Wilton Park focused on the questions of how the UK financial services industry can act better collectively in this next phase of deepening cyber resilience. The UK landscape already contains many effective forms of collaboration. However, prior attempts at comprehensive initiatives have lacked a strategic business case, have been undermined by a lack of trust that inhibits information sharing and have lacked urgency and top-level buy in.

22. The new body should be led by the private sector but leverage established links with law enforcement, the Home Office and other relevant government agencies. It also needs to build on established links with financial regulators, though this must be developed in a way that generates mutual trust and allows firms the scope to discuss resilience without direct supervisory oversight.

23. Such a body needs a robust business case and support at the highest level of industry. It should cover the entire sector but start with and focus on critical national infrastructure. It needs a focused and limited agenda that can expand with proof of concept and developing confidence and trust. Its initial focus should be on:

    - Central intelligence coordination;

- Real time tactical and threat intelligence sharing across the sector, with contextualisation and support for smaller firms;
- Best practice in cyberattack playbook design, with a mission to help disseminate best practice across the sector, including to smaller firms.
- Outreach to key third party providers in the fintech and telecoms sector with a long-term aim of deepening and maturing the financial sector's collaboration of cybersecurity with the service providers on whom it depends.

Stephen Adams, Conan D'Arcy, Franck Thomas
Wilton Park | November 2018

Annex: the Wilton Park agenda

The UK financial services sector is on the front line of the challenge of cyber-crime. This is compounded by the sector's changing digital profile and the evolving nature of the threat. Attendees at Wilton Park agreed five core responses:

A new collective discipline of cyber resilience planning	• Continually improving mapping of service continuity and systemic risk impacts of cyber- attacks, including beyond the FS sector itself. • Refined firm and sector level definitions of tolerance for service disruption and recovery • Continued sharing of best practice in cyber-resilience and cyber-attack playbooks, especially between large firms and smaller ones. • Regular firm and sector level contingency planning exercises, with results systematically iterated with playbooks
Better intelligence sharing	• Move from 'one-way bilateral' model of intelligence sharing between firms and law enforcement and regulators to one in with clearer feedback and greater use of intelligence laterally across firms engaging with law enforcement to maximise benefits. • Review of legal frameworks for sharing customer data in pursuit of cyber-resilience measures and action where necessary to clarify liability framework. • More focus on supporting less sophisticated firms in escalating threat intelligence and contextualising and interpreting threat intelligence being disseminated to them.
A deeper cyber risk culture in firms – from practitioners to Boards	• Continued focus on developing cyber-resilience as a business-wide discipline; augmenting technical skills with skills in communication, firefighting and risk interpretation. • Continued focus on developing executive competence in understanding interpreting and directing cyber-resilience activity. • Focus on the skills gaps in cybersecurity, especially encouraging a strong pipeline of young professionals and taking a collective view of the value of a deep pool of skills in the UK.
A new dialogue with the public	• Develop new tools for communicating to the public the level of cyber threat, the effectiveness of cyber resilience activity and the necessary acceptance of occasional breaches. • Resist any temptation within the sector to emphasise peer weakness as a competitive advantage.
A new body to drive industry resilience and collaboration	• Develop a new body to drive industry-level efforts on the themes above.