BANK OF ENGLAND

Speech

Stock-take of global cyber security regulatory initiatives IMF cyber security workshop

Speech given at

IMF cyber security workshop by Lyndon Nelson, Deputy CEO of the UK PRA, Bank of England and Co-Chair of the G7 Cyber Experts Group

5 December 2018

At the outset, I would like to offer my thanks to Jennifer Elliott and Nigel Jenkinson for inviting me to speak on this important topic. I should also like to congratulate the National Bank of Belgium for their continued sponsorship of this event and for their wider support of technical assistance for lower income and developing countries. It is indeed an honour to be asked to be part of this very noble initiative.

The Bank of England and the G7 Cyber Expert Group recognise the importance of events such as these in building resilience not only in our national silos, but to impart our knowledge and experiences with the global community.

I've been set the task of informing you on current and future regulatory initiatives that are progressing across a range of international multilateral groups focused on cyber security. One could call this a "State of the Cyber Nation" address, which is international by its very nature given that cyber knows no borders.
This will, of necessity, be a whistle stop tour, in which I hope to cover my thoughts on: the cyber threat landscape; the vulnerabilities which make the financial sector susceptible to cyber risk; some of the common challenges which we've encountered both domestically and internationally along our collective cyber journey; and just at the point where I will have you the most worried, I will cover what the international regulatory community is doing in the face of these risks.

Threat assessment

In my role as the co-chair of the G7 Cyber Experts Group, I have been reaching out to a number of non-G7 countries, listening to their challenges and learning about their response. During the course of these engagements I have picked up a number of local idioms which have been used at one time or another in the presentation of the local cyber environment. In an effort to make my speech today "more international" I hope to sprinkle my remarks with some of the more evocative idioms that have been presented to me.

By far the best idiom to describe the current state of the threat comes from Sweden who told me 'det finns en ko på isen', which translates to "there is a cow on the ice". Much like this fictitious cow, the financial sector is in a precarious position, facing a clear and present danger from a range of cyber threat actors. But first, let us think about the common characteristics in cyber shocks, which distinguish them from other operational shocks.

- Intent. Disruptive attacks are conducted with malicious intent, designed to inflict maximum damage perhaps by combining attacks on multiple systems, or by selecting a critical date.
- Probability. It is widely accepted amongst experts that probability of success is now much higher and a higher impact event is a matter of "when" rather than "if".
- Timing. The attack might involve a hidden phase, where malicious code is inserted and data compromised and/or manipulated to create problems. Once the attack becomes known, it can be difficult

to appreciate the extent of the damage and to identify effective solutions. As an example, experts believe that the 2017 NotPetya virus had been present for several weeks in targeted hardware.

- Adaptability. New tools and techniques available to cyber attackers reduce the cost of attacks and heighten the impact, whilst at the same time increasing the cost of defence. They also enable attackers to exploit previously untapped vulnerabilities.

The most common and prominent adversaries consist of a multitude of cyber criminals using stolen credentials or confidential data to perform fraudulent activity. This could be regarded as a traditional threat, fortunately, these criminals are less motivated by disruptive or destructive objectives, as they equally rely on a functional financial system to derive their illicit gains. Their capabilities range from low skilled opportunists using unsophisticated techniques through to highly organised, sophisticated crime-groups operating across international borders. At the other end of the spectrum, are nation states, who can use a variety of techniques to achieve their aims. In my opinion, there is a distinct possibility that state or state-sponsored actors have or will seek to compromise financial institutions for the purpose of economic espionage, theft of intellectual property for commercial advantage or to destroy or corrupt systems for political or strategic gain.

A relatively new development is the phenomenon of more sophisticated actors selling their knowledge and toolsets to less sophisticated threat actors. The rise of crimeware as a service (CaaS) enables new entrants to conduct malicious cyber operations with limited technical understanding. Such services allow off-the-shelf tools to be readily purchased to conduct denial of service attacks, steal financial information, or deliver malware. In addition, some nation states seek to leverage elite cyber criminals aligned to their strategic ambitions in a coalition, providing the cover of plausible deniability. The age of the 16th and 17th Century privateer - a pirate for hire has found a new and more modern manifestation.

Corrupt or subverted insiders represent one of the most capable threat actors facing financial institutions, given their access to valuable internal information processes. Insiders may be financially or ideologically motivated to conduct an attack or even coerced by capable threat actors seeking lucrative targets. Covert data exfiltration, deliberate disclosure of sensitive data and fraudulent transactions are examples of potential malicious activity.

As defences improve across the globe, adversaries require greater investment of time and resources to achieve their goals. As a result, their focus shifts to softer targets and geographies with comparatively weaker security and audit controls. As the famous joke goes, two friends are walking in the woods and one turns to the other. "If we get too close to a Bear do you think we can out run it?" "No", says, his friend, "but I only need to out run you."

So, the financial sector is a veritable cash cow, and the ice is thinning.

Vulnerabilities

Switching to vulnerabilities now, and this time drawing on the Chinese for inspiration: "Wú fēng bù qǐ làng", or "without wind, you cannot have a wave." There is little that the financial sector can do to change the nature and scale of the cyber threats it faces directly, that is the responsibility of law enforcement and other government authorities. However, a threat without a vulnerability is not a concern. Whilst it is therefore important to note that financial authorities and institutions should remain threat aware, they should spend more time and effort identifying, understanding, and addressing their cyber security vulnerabilities.

In financial stability terms, there are broadly two types of vulnerabilities that make the finance sector susceptible to cyber risk. First, there are common individual vulnerabilities, observed at a wide range of financial sector entities. To the extent that these can be exploited, they represent a systemic risk, as a given cyber incident could affect multiple firms and the financial infrastructure on which they rely. Second, there are systemwide characteristics, specific to the financial system that makes it susceptible to widespread damage and disruption (with potential for dislocation of the real economy), arising from a major cyber event.

In principle, individual entities should have strong incentives to mitigate these vulnerabilities, as they affect their own resilience, as well as that of the system as a whole. But the common prevalence of a wide range of vulnerabilities suggests that the private incentives of financial institutions may not be fully aligned with public incentives. For example, institutions may not allocate sufficient resources to cyber security, or they may be disinclined to share information with other entities in the event of a cyber incident. Assessments across the globe carried out by supervisors highlight recurring and prevalent weaknesses, four of which I will describe:

- Insufficient cyber strategic planning and influencing. The effectiveness of cyber resilience measures are undermined by deficiencies in board level influencing, organisational design, operating model and strategy. A strong example of this is the thematic underinvestment across the sector in the security culture.
- Insufficient industry oversight of third-party suppliers and supply chain. Firms in the sector tend to have an inadequate approach for oversight of their supply chain and third parties that often provide their information processing or IT systems. I will cover this item in more detail when I cover industry challenges.
- Ineffective testing of people processes and technology. The sector as a whole does not conduct adequate effectiveness testing of cyber across people, processes and technology. Assurance is largely gained through audits and control sampling which is not sufficient. Sampling by its nature is partial, whereas cyber defence often needs to be looked at holistically.
- Inadequate cyber hygiene. Cyber hygiene, which involves having basic and core practices and processes in place to improve cyber security, is not yet consistently followed in some firms. Examples of hygiene issues include shortcomings in vulnerability management and information storage, poor configuration of

IT infrastructure and poor user account and password management. These issues are exhibited by both large and small firms and those from across the full range of IT infrastructure in terms of size, complexity and budgetary resources. It is this inadequacy of cyber hygiene that lies at the root of over 80% of the successful cyber attacks on firms.

I have called these the vulnerabilities of omission as they stem from insufficient, inadequate or ineffective execution. In addition, there are vulnerabilities that arise from the very nature of the financial system itself but may equally be used and exploited in cyber attacks. There are certain system features that – in a cyber context – could exacerbate the impact of a vulnerability being exploited. At the same time, these features may serve the financial system in important ways (for example central counterparts offer significant financial risk reduction benefits).

- A high degree of interdependence both between financial sector entities and organisations outside the financial sector. Some of these dependencies arise from the use of common financial service providers (for example, correspondent banking and central counterparties), others from relying on common technologies and applications. In some areas, we observe high degrees of concentration (for example, power and telecommunication services) and limited substitutability (for example payments and settlement systems).
- A lack of transparency regarding the interconnectedness and concentration within the financial system. Similarly, there is a lack of transparency and understanding of the critical infrastructure upon which the delivery of financial services is dependent.
- A sector reliant on data, often sensitive and time critical hence a loss of data integrity (data being corrupted), data confidentiality (unauthorised access) or data authenticity (creation and spreading erroneous data) could have a significant impact on a wide range of financial services (for example trading or insurance). In some instances, data damage or losses may go undetected for a long period of time.
- A sector reliant on confidence. Confidence (or trust) can vanish quickly as witnessed in previous financial crises. For example, a severe cyber-related outage at one or more retail banks could affect trust and deposit taking more generally. As such cyber incidents could (intentionally or unintentionally) undermine confidence in financial sector entities or functions. Trust may also be weakened if market participants become aware of a cyber-related data breach that had been undetected for a long period of time.

These are just a few examples. In short, we cannot fix what we do not know. Understanding our frailties is critical, if the financial sector is to survive and thrive. The lesson being that we "need to see which way the wind blows" before we can "ride the wave".

Challenges

Neither the financial sector nor its regulators stand still and this creates both opportunities and challenges in a cyber context. But as the Germans would say: "es gibt leichen im Keller", or "there are corpses in the cellar". In the following examples, we have seen advances with a range of potential benefits, but which reveal pitfalls on closer inspection.

- The rapid growth of outsourcing and the use of third parties. Outsourcing has sometimes been motivated by cost and efficiency and in other cases to achieve improvements in the management of risk. These days, many of these third parties are entities that are outside of the financial system. Like all outsourcing they create new dependencies in which the financial system must rely. Indeed, in some instances, firms are now entirely dependent on third party providers. Furthermore, in some areas there are significant concentrations with many firms relying on one or a small number of third-party providers. Whilst regulators expect firms to manage the risks associated with outsourcing, managing this concentration risk is a challenging task. Especially when there are no ready substitutes, the power to negotiate is limited or substitution is insufficiently tested. From a cyber security perspective, an organisation supply chain represents a significantly preferred attack vector for advanced threat actors. Adversaries take advantage of trusted third-party relationships to deploy a range of tactics, from targeting IT outsourcing companies stealing client data from their systems for espionage, to manipulating and "poisoning" legitimate software to allow destructive malware into networks.
- The Cloud. From a UK perspective, we have seen a huge increase in the number of firms considering a move to the cloud. Outsourcing to the cloud offers significant cost and risk reduction opportunities. If configured correctly, it can provide resilience benefits to individual institutions, because the scale of cloud service providers allows them to build resilience in a way that exceeds the investment capability of individual firms. Notably the Cloud sector is highly concentrated. At the global level, Amazon Web services dominates the market, accounting for around 40% as of the first quarter 2018. Together, the top three firms, Amazon, Google and Microsoft, account for just over 60% of the market. The concentration of cloud service providers is a concern; not only for the contagion effect if disrupted, but given they represent a very tempting target to any threat actor. Customers need to fully understand the implications of the shared responsibility model and the distinction of security of the Cloud versus security in the Cloud. For the avoidance of doubt, customers are responsible for the latter. It requires an implementation of business and application segmentation according to zero trust principles (never trust, always verify), and maintaining an agile security approach to face off against highly dynamic workload allocations. Failure to understand these principles could lead to a weakened security posture post-migration to the Cloud that can put important data and intellectual property in danger.

- Plethora of standards. Cyber security regulations have proliferated over the past few years as the significance of the threat is draw more attention. According to last year's FSB stock-take, 72% of jurisdictions reported publicly releasing plans to issue new regulations, guidance or supervisory practices that address cyber security for the financial sector in 2018. Regulations are necessary, and will inevitably and justifiably diverge where different governments view the need of their citizens differently. But for global firms, this can result in an international patchwork of requirements, standards and potential liabilities if they don't get it right. The patchwork of rule making can lead to counter-productive outcomes, with new cyber security standards overlapping with multiple existing standards, without any empirical analysis of actual effects. Rather than improving cyber security, such incongruence may divert to unproductive compliance processes the very resources the entities could otherwise devote to securing operations.
- Information exchange. If there is one topic which is more prevalent in international cyber forums than even "regulatory fragmentation", it would be "information sharing". On the surface, it may seem innocuous and a positive activity to engage in, but the devil, as always, lies in the detail. The term itself may be widely used, or indeed misused, to cover a multitude of scenarios. Unless there is clarity and what kind of information or knowledge is to be shared, for what purpose, between which parties, by what means and more parameters besides, the end result is invariably differing interpretations and expectations. This all presupposes a desire to share in the first place, which is by no means certain with the prevailing geopolitical climate. Sharing is inexorably linked with trust, which is slow to build and can be lost in an instant. Even if the will is there the challenges of quickly interpreting a cyber incident such that meaningful communication can take place are very high.

These are just a sample of the challenges which we face domestically and across borders when it comes to cyber security. As mentioned earlier, it's useful to understand where the "bodies are buried", because only then can we build solid foundations upon which the financial sector can rely.

If you have made it this far I have good news. This concludes the "doom and gloom" segment of my speech, where the world's ills are laid bare. It should come now as some relief to hear about all the various ways in which the international community is trying to address at least some of these issues.

The landscape

When I spoke at last year's IMF cyber security workshop, I describe the rapid proliferation of international bodies discussing cyber security, resulting in a somewhat fragmented and at times duplicative landscape. 12 months on, I can report that the formation of new groups appears to have abated, constrained by the availability no doubt of authority resources to commit towards international engagement. Existing groups are beginning to mature, looking outwardly to minimise overlap and receiving greater scrutiny over their mandates. As the Portuguese would say: "quem não tem cão caça com gato", or "he who doesn't have a

dog hunts with a cat". In other words, these groups are reaching the limits of what they can do with the resources they have to hand. Necessity however is the mother of invention and I've seen much greater collaboration between these groups in the last year.

What has not changed however is the limitation imposed by the "circle of trust". With heightened cross-border tensions, and some jurisdictions becoming more tribal, there is a recurring preference to collaborate based on pre-existing relationships. This can be an impediment to larger multilateral forums, where political positions can take precedence over the desire for financial authorities to work together. Finding the common, nonsensitive ground to discuss cyber security issues continues to be an ongoing challenge.

G7 Cyber Experts Group.

Despite these obstacles, cyber remains a "hot topic", fuelled by continuous media coverage of incidents, speculation and technical developments. Cyber is also expected to feature highly on both the G7 and G 20 presidency agendas for 2019, under the headings of "effective multilateralism" and "fragmentation" respectively.

As co-chair of the G7 Cyber Experts Group I'd like to provide you with an insight into both the groups recent efforts and future direction. No doubt you are already familiar with our first publication from October 2016, the "Fundamental Elements Of Cyber Security", which encapsulates effective practices on cyber security for both public and private financial sector entities of all sizes. It is the bedrock upon which the ensuing Cyber Expert Group work has been built. However, you may be less familiar with the three subsequent fundamental elements now in the public domain, covering effective cyber assessments, third-party cyber risk management, and threat-led penetration testing. Each set of principles extends the original fundamental elements on topics which G7 finance authorities considered a priority for building common and consistent understanding.

On third parties, the cyber expert group identified a need for baseline hygiene factors to management of external relationships, and the consequences for cyber risk in both a firm specific and systemwide context. The G7 publication on threat-led penetration testing aims to foster convergence on an emerging practice, and create a critical mass to which others can gravitate towards. Aside from providing the key considerations for any public or private entity which wishes to undertake this type of testing it provides a basis for mutual recognition and equivalence discussions. By including a process of accreditation it fosters the supply of a highly skilled workforce that can be available to everyone.

To complement its thought leadership output, the Cyber Expert Group also provides a forum for G7 authorities to develop their collective operational capabilities. Most notably, the Cyber Expert Group is facilitating a cross-border simulation exercise in 2019, which explores how 23 authorities would communicate

and coordinate in the face of a significant cyber incident. The group will examine the consequences of a multi-day disruption resulting at a GSIB which may be financially viable, but operationally disabled.
One of the recurring questions I receive is where should the cyber expert group focus its attention next? To address this point, as part of our new mandate, the Cyber Expert Group will seek to establish a collective view of vulnerabilities which it can then use to prioritise its future work stack. This will be a challenging effort, requiring reconciliation of both authorities and industry perspectives on gaps or weaknesses which are prevalent or shared. Are these vulnerabilities systemwide or structural in nature? Are the vulnerabilities we perceive merely manifestations of an underlying root cause which needs to be addressed? How do we minimise the "urgent" pushing out the "important" as is often the case? These are just some of the questions that the Cyber Expert Group will have to grapple with over the coming months.

Industry engagement is often regarded as essential as part of international initiatives. It is relatively easy-to-use the convening power of financial authorities to invite or indeed "compel" industry to participate in dialogues, presentations or question and answer sessions. However, this approach fails to harness the power of collective action, where identification of issues and the efforts to address them are shared across the public-private divide. The Cyber Expert Group is maturing its relationship with industry in this direction, with three core principles in mind:

- first, industry representation at Cyber Expert Group meetings is not sourced from individual institutions. Individuals are selected by each G7 jurisdiction on the basis that they represent domestic collective action forums, with cross sectoral coverage. In the majority of cases, industry chairs for these forums are nominated to attend the cyber expert group. Sometimes, these arrangements can have unintended, but positive consequences. For example, the industry chairs noted that they themselves had never met, so the Cyber Expert Group provided an important networking opportunity for industry to work across borders;
- Second, we want to shift industry engagement from peripheral to integral. Ultimately, we seek to create joint products by embedding the private sector from the very outset. Indeed, for some of our challenges we have concluded that an industry led approach is often preferable. Imagine for example, the issue of intelligence gathering of vulnerabilities across the financial system. The collective database of these vulnerabilities would easily be one of the most prized data assets for any attacker to go after. Therefore, the traditional regulatory approach of regulator collecting data potentially creates a significant additional vulnerability;
- third, industry can act as an amplifier for the Cyber Expert Group's work both in terms of the resource pool that can be leveraged, and in spreading the message still further.

Other international developments

Aside from the Cyber Experts Group, I would now like to spend some time on other notable international developments which delegates should have on their radar. I'm conscious not to pre-empt content from the subsequent panel session, so I intend to provide a preview and a synopsis, which my fellow speakers can describe in more detail.

Following its 2017 stock-take of regulatory and supervisory practices on cyber security, FSB members had to determine what further activity could be undertaken. The key observation arising from the stock-take was the inconsistent use or understanding of key cyber terms even across FSB members. Therefore, as a first step towards building common understanding, the creation of a Cyber Lexicon was born. Careful not to reinvent the wheel, the Cyber Lexicon leverages existing definitions from international standard setters such as ISO or NIST, with minimal adjustments. The end result is a glossary of just over 50 core cyber terms and their definitions which FSB members can leverage for domestic and cross-border policy or capability development, and in public communications. A good example where the lexicon process has been useful is in terms such as "cyber attack". Despite its common use, the term was hotly debated at the international negotiating table, well beyond the bounds of the financial sector. The latest version of the Talinn Manual considers a cyber attack as "a cyber operation that is reasonably expected to cause injury or death to persons or damage or destruction to objects". Clearly a much higher bar than when we might use a cyber attack to describe a denial of service campaign or exfiltration of data. The term also brings with it the concept of attribution, which becomes the purview of law enforcement, rather than financial authorities. As a result, the Lexicon sidesteps this issue by expanding the non-sensitive definition of "cyber incidents" to indicate that it could arise from malicious circumstances or not. Speaking for the Bank of England, this approach aligns with our "cause agnostic" perspective that focuses on impacts from operational disruption irrespective of their origin. We expanded upon this approach in a recent discussion paper on operational resilience. With the first edition of the Lexicon published on 12 November, FSB members were back to the drawing board revisiting the "what next?" question. After further deliberation, members have agreed to focus their efforts on how financial institutions (individually or collectively) respond to, and recover from, cyber incidents.

The Basel Committee's Operational Resilience Group is, as the name would suggest focusing on broader operational resilience, inclusive of cyber risk. Initially, this will entail definitional work, and review of existing BCBS standards and guidance. The subsequent gap analysis will form the basis for recommendations to update the "principles for sound management of operational risk". The ORG will also compare jurisdictions existing resilience assessment tools and methods and explore opportunities for standardised metrics.

The IAIS financial crime task force has recently published a draft "Application Paper on Supervision of Insurer Cyber Security", leveraging the G7 Fundamental Elements, and expanding them to provide an insurance supervisory perspective.

It has been two years since CPMI-IOSCO's seminal and often referenced "Guidance on Cyber Resilience for Financial Market Infrastructure". The group responsible for this publication has been evaluating adoption and conformance to the guidance via respective oversight functions, as well as investing in outreach opportunities to a global financial market infrastructure audience.

There are also regional developments of note from the past 12 months to bring to your attention. First, it's been a busy year for the ECB as they completed the first round of their cyber triage questionnaire covering 39 payment systems across the EU, and formally releasing their EU wide threat led penetration testing framework known as TIBER–EU. And still not content with that, the ECB has also released "Cyber Resilience Oversight Expectations" for public consultation.

In the US, the "Financial Services Sector Cyber Security Profile" is the product of a two-year industry led initiative to improve operational efficiency in response to a fragmented regulatory landscape the profile is a meta-framework organised to align with NIST framework categorisation whilst drawing upon, and mapping to, major standards and guidance. The profile promises to reduce the time a financial institution needs to complete a comprehensive assessment by combining overlapping expectations from multiple regulatory organisations, and offering a tailored set of diagnostic assessment questions, reflecting an institution's risk to the broader economy. The European Banking Authority has also issued guidance on cloud outsourcing.

Operational Resilience

I will end my tour of landscape developments with the emergence of the next hot topic to follow cyber. Although embryonic within the financial sector, this concept captures the operational outcomes we seek as authorities in the same way that we would for financial resilience. Cyber security is also a key element to operational resilience. As we have seen in recent years, adversaries can have the properties of a liquid, finding every crack and gap in a firm's defences and settling at the level where there are the fewest controls. These weaknesses can be related to gaps in process, technology, people, skills or awareness. The cyber threat brings operational resilience into greater focus and requires organisations to understand themselves, their strengths and their weaknesses. It becomes essential for firms to understand their most critical assets and their most critical functions. What defines critical? Well, several things: the importance to the customer; the importance to the integrity of the firm; and the importance of the sector and the wider economy. Armed with this information they can then allocate their finite resources in the most targeted way. Consider this is a trailer for tomorrow's session on this very topic by my colleague, Nick Strange.

Looking forward

In a speech earlier this year, I urged regulators and industry to be on a WAR footing. Firms should be able to Withstand attempts to penetrate their systems. They should be able to Absorb attacks when they take place. And they should be able to Recover their functions as quickly as possible.

I offer three medium-term predictions, with the Japanese caveat that "even monkeys fall from trees". In other words, even experts get it wrong.

- Across international cyber groups, collective understanding will mature and thinking will coalesce, driven by greater collaboration. We do need to remain vigilant to groupthink given that many of the same individuals maintain roles across these various fora. To my mind it also means that thought leadership should focus on principles, rather than prescription, leaving individual jurisdictions and institutions the flexibility they need to determine how they meet consistent outcomes.
- As I have said in the past, cyber incidents will occur. And these will become more frequent and disruptive, unless firms and sectors as a whole develop the adaptive capacity to absorb the shocks whilst continuing to deliver the services that matter most. The shift towards a resilience mindset has already begun, and will become the foundational pillar of future cyber regulation and supervision.
- As an industry and society, we will reach "peak complexity", where our ability to understand the intricate interdependencies of complex systems will be beyond our reach. We cannot protect what we do not comprehend. I foresee a reaction response in the form of a sustained and emphatic drive towards simplicity.

And lastly, if I may, a direct appeal to my audience today. Some key suggestions for you to take away and begin to implement.

- Stay informed, and leverage the work of others. Little of what is done internationally on cyber security remains behind close doors, and is publicly available for your benefit.
- Start small and build capability gradually. Better to establish and become more familiar with foundational concepts first, than overstretch, underachieve and lose confidence.
- Focus on recovery as much as prevention. Operational resilience begins where operational risk ends. It starts with a mindset that an event has occurred and then asks the question how do we respond?
- Work with each other. This is a shared problem, where many of you will be struggling with near identical issues in similar circumstances. Workshops such as these should only be seen as the start.

And finally, do not hide behind the excuse that you need sophisticated cyber resources in order to make progress. 90% of the work on cyber does not need technical expertise in cyber. It needs the understanding of people, processes, and data as much, or in fact more than, technology.

This concludes my "State of the Nation". There is still much to do, but I'm happy to say that in the issue of cyber resilience, I continue to find a highly collaborative approach that means progress in combating this issue has and will continue to be rapid. Alas given the nature of the threat, it will need to be.