BEYOND blue

SUPPLY CHAIN *RESILIENCE*

Complex, Interdependent and Systemic

THE CHALLENGE

It is tempting to focus on the management of risks within the boundary of a single organisation where we can establish governance and culture, create systems and controls, audit and monitor compliance. Our world is now far more complex that that, with dependencies on an ecosystem of partners and suppliers, giving rise to challenges of systemic risk associated with the critical nodes within that ecosystem.

Our approach to managing resilience demands we engage with many third parties who may not share our culture or incentives, and certainly not our systems and processes. The world of cloud, software as a service (SaaS) and open application programming interfaces (API) – challenges us to rethink our approach to risk and resilience.

The changing pattern of cyber attacks we have seen over the last 5 years shows that organised crime (and indeed States) are alive to this issue, and willing to exploit our dependencies for financial and political gain.

In 2017, the destructive wiper malware known as NotPetya struck several unsuspecting firms despite their maintaining costly in-house security operations and controls. The initial vector for the attack? The compromise of a tax and accounting software package little used outside the Ukraine produced by a small-to-medium sized enterprise. In the case of shipping giant Maersk, all it took was one infected Odessa based system connected to the corporate network to compromise much of their global network. In total, the NotPetya compromise cost Maersk somewhere in the region of $250-300 million.[1]

Likewise, in 2020 it was revealed that Russian hackers had successfully introduced a backdoor into the Orion software system of SolarWinds, a major IT firm with some 33,000 Orion users as customers.[2] Included amongst these were Microsoft, Cisco, Intel, Deloitte, and various US Federal agencies.[3] Alongside reputational damage, the affected organisations were left with the uncertainty surrounding whether sensitive company data had been exfiltrated and whether their systems were secure or not.

Of course, technology failures also play their part, with configuration changes to complex technology causing surprising levels of disruption. Facebook's outage on the 4th October 2021 was attributed to a routine maintenance job which resulted in a command being issued to assess capacity on their global backbone. That, well intentioned, command took down the whole Facebook global backbone and disconnected all of their data centres. Fault finding and diagnostics when the network is down is hard, and so was physical access to some of the data centres sites. Restoration of complex and interdependent services takes time, and so it did for Facebook, and for many firms who depended on their services.

While isolated cases, these do illustrate a broader trend toward malicious supply chain attacks which sits alongside other cases in which systemically important infrastructure is disrupted or fails for a wide range of reasons from technology failure to human error.

[1] Olenick (2018) [2] SEC Form 8-K (2020) [3] Sjouwerman (2021)

THE ECOSYSTEM

The financial services (FS) sector is more highly interconnected than most sectors, both functionally and technologically. Most FS firms have come to depend on a common set of third parties for critical functions, notably payment, clearing and settlement through financial market infrastructure (FMI) providers. Market data services, advanced analytics and real time trading platforms have been a key part of achieving a competitive advantage for investment banks; while FS firms seek to keep pace with the dizzying array of disruptive new services and technologies commonly grouped under the umbrella term "Fintech".

The outsourcing of critical IT and data management service functions to managed service providers (MSPs) is well advanced, including the outsourcing of a wide range of fraud and transaction risk scoring services, and even (and perhaps ironically) security operations services themselves.

The result is a sector in which supply chains, or more accurately, supplier ecosystems are ever more complex; and the challenges of understanding and managing risk and resilience increasingly demanding. More than that, the concept of substitution of services in its infancy, whether that is the portability of cloud workloads in multi-cloud environments, or a diverse payment infrastructure, or modularised APIs which allow plug-and-play of data and analytic services. The tension between harnessing innovation (with associated lock-in) and resilience through diversity of substitutable offerings is stark.

THE DILEMMA

At the heart of these questions and the related problems surrounding FS supply chain risk is a simple prisoner's dilemma. Every firm at every tier has a vested interest in lowering the overall risk across the supply chain. But they also want to minimise their own obligations to expend resources on what they likely see as somebody else's responsibility. No firm wants to have to invest its own resources to prevent the emergence of negative externalities which arise due to the failure to manage risk by some other node of their supply chain.

This is further complicated by the significant imbalances of power within the supply chain, and very different approaches to risk and resilience management. A systemically important bank or FMI provider is likely to have a well-resourced, advanced and enterprise-wide approach to risk management, and sophisticated security operations. They have significant financial leverage on their supply chains when compared to smaller parties. But the real picture is more complex. They often interact with equally powerful (or more so) large technology service providers, monopolistic market data providers who cannot be easily replaced, and market leading FinTechs with highly attractive and innovative offerings. Each of these categories of firms have very different risk and resilience approaches. So, the scene is set for a complex and potentially adversarial power game.

THE REGULATIONS

Most large UK financial institutions are grappling with the recently released Operational Resilience regulations from the PRA and FCA. In particular, the obligation placed on institutions to understand the resilience of their third parties in the case of a range of severe but plausible disruption scenarios. A deliberate counterpoint to conventional risk-based approaches which consider likelihood and impact, and often focus on the preventative controls which reduce likelihood rather than the impact mitigation measures which reduce either the time to recover or the harm caused by the outage to customer and clients. This regulatory obligation adds to an already complex set of obligations flowing from previous material outsourcing and third-party risk management regulation.

So how then can financial institutions satisfy themselves of the resilience of their supplier ecosystem, and what behaviours might this quest for confidence generate in the actual resilience of that ecosystem?

THE MODELS

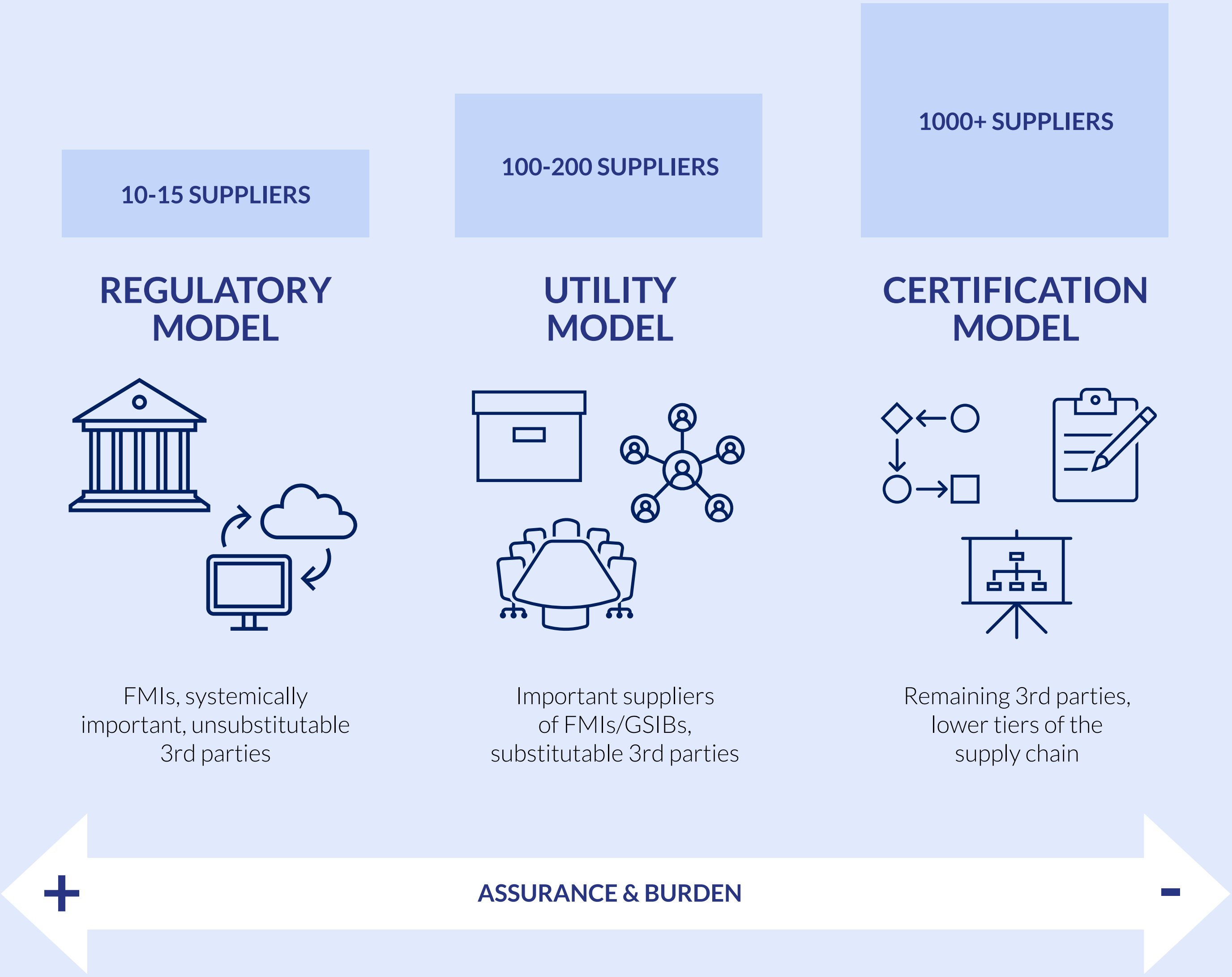
Of course, financial institutions can seek to demand assurance from their suppliers directly, perhaps including these obligations in changes to standard contract terms. In doing so, the power game plays out. The big financial institutions will success in "arm twisting" suppliers, but the larger suppliers will push back against the multitude of different approaches they will receive as every financial institution attempts to enter into dialogue. So, is there a better way?

Of course, one option is that the supplier ecosystem be brought under the same **regulatory model** as the financial institutions themselves, allowing them to rely on the effectiveness of that regime. This seems wildly unrealistic for all suppliers within the ecosystem, and perhaps for all but the most systemically important of those suppliers. The attempt to impose such a regime, with associated overheads, is also likely to be disproportionate and costly, while potentially also erecting barriers to entry to the UK market. Nevertheless, the Treasury has signalled its intent to explore the regulation of critical third parties which are systemically important to the financial services sector. The Department for Digital, Culture, Media and Support (DCMS) is also consulting on the potential extension of the Network and Information Systems (NIS) regulations to MSPs also, which will also involve discussions on quite how they set the materiality criteria for which MSPs are included with the regulatory scope. And finally, FMIs are already regulated, although regulators have been robust in stating that financial institutions must still satisfy themselves of their resilience irrespective of the fact they are directly regulated.

A second model has been explored – **the utility model** – in which supplier assurance is provided through the use of centralised risk monitoring and management platforms. Examples include the Hellios financial services qualification system (FSQS) and S&P Global's know your third party (KY3P) platform. These platforms provide a centralised data hub populated with up-to-date risk information on suppliers' control posture, based on a comprehensive assurance process which

seeks to meet the requirements of most organisations. Of course, some financial institutions will continue to have unique or unusual requirements, but these platforms seek to deliver an 80-20 solution. While their due diligence and assurance offerings are developing, they differ in philosophy from the scenario testing approach enshrined in the operational resilience regulations by focussing primarily on suppliers evidencing whether individual controls are in place.

The third and final model is – **the certification model** – in which suppliers are assessed against an externally defined standard. Of course, these include the American Institute of Charted Public Accountants (AIPAC)'s System and Organization Controls (SOC) standard, or a wide range of international standards such as ISO 27001 and ISO 22301, the UK government's Cyber Essentials standard, or the cyber assessment framework (CAF) developed in support of the implementation of the Network and Information Systems regulation for critical national infrastructure. Typically, certification will be undertaken by an accredited certification body, and many consulting firms position themselves to provide such services. Again, we have the challenge that resilience standards are still in their infancy, and while ISO 22301 provides a framework for business continuity process assurance, this does not cover the full scope (or indeed philosophy) of the operational resilience regulations.



10-15 SUPPLIERS

REGULATORY MODEL

FMIs, systemically important, unsubstitutable 3rd parties

100-200 SUPPLIERS

UTILITY MODEL

Important suppliers of FMIs/GSIBs, substitutable 3rd parties

1000+ SUPPLIERS

CERTIFICATION MODEL

Remaining 3rd parties, lower tiers of the supply chain

THE ANSWER?

Perhaps the answer is a hybrid approach, and one which will evolve as our experience of implementing the regulations develops. It seems clear that a growing number of systemically important firms will come under direct regulation. That regulatory framework may be a critical third-party framework focussed on the needs of the financial sector, or a MSP assurance regime under the NIS regulations, or indeed a mix of both. Either way, regulation of those firms now seems inevitable, along with growing pressure from the financial institutions to whom they provide services.

We also expect to see the development of new utility models, or the extension of existing utility platforms to encompass a broader operational resilience assurance model. Small steps are being taken at the moment, for example the Cross-Market Operational Resilience Group (CMORG) is sponsoring a proof of concept to explore collaborative scenario testing of systemically important firms. This proof of concept is exploring whether the FS community can arrive at a common scenario testing approach to assess the resilience of those third parties. In effect, running a set of scenarios with the third party to understand their resilience approach, recovery assumptions, and likely recovery timescales. This may in turn help explore whether we can generate sufficient consensus around the test methodology and subsequent findings to make it viable cross-sector as a useful way of providing assurance evidence to the community. If successful, it may well find a home as an extension of the offerings of existing utility platforms – in effect a third-party scenario test service. Ultimately, this may reduce the burden on suppliers of multiple and diverse customer requests.

Can we go further? The regulatory model may only apply to a dozen entities, the utility model to perhaps a hundred suppliers who are widely used across FS... but beyond that what do we do about the broader community?

It seems we need to look to the certification model, or perhaps other constructs to scale. Independent audit has the potential to scale but requires time to establish the accreditation and certification frameworks, and build the base of certifiers. For example, the UK Cyber Essentials scheme now certifies tens of thousands of firms, albeit with a relatively straightforward assurance model. That scheme was launched in 2014 and has been scaling up ever since. There seems to be a role for an evolved assurance standard, and the subsequent build out of the certification model. Ironically, we may find that financial institutions themselves come under pressure to demonstrate to their clients that their resilience approach is also robust, so they may themselves be candidates for such independent assurance. Of course, we may find that self-certification is the first step along this path, but that will still require a de facto or de jure standard as the basis of that self-certification, which again implies community effort to develop that consensus view.

THE COMMUNITY

Ultimately each of these models should seek to drive improved resilience across the community, but will firms have the capacity or skills to meet the demands of these assurance or regulatory interventions?

We also need to consider community capacity building. The role of the large firms in helping their supply chains and the community supplier ecosystem build resilience by upskilling and by sharing best practices. In a previous life, I established the Defence Cyber Protection Partnership (DCPP) at the Ministry of Defence. It's aim was both to ensure that MOD's prime contractors sent consistent signals to their supply chains over the need for cyber security, but also that they worked with those suppliers to help them in meeting the MOD's requirements. It brought the community together to discuss how to align communications, contract expectations and support initiatives. Perhaps a similar approach will be needed across the FS sector in the UK – a role for UK Finance perhaps?

THE NEXT STEPS

Over the next 12 months it is clear that implementation of the PRA and FCA operational r esilience regulations will continue to occupy the mind of financial institutions in the UK, and with that there will be growing pressure for a co-ordinated approach to third party and supply chain resilience for the sector.

Expect regulatory action for critical third parties shortly, but also expect to see the utility model and certification models develop over the next 12-24 month as financial institutions begin to align around requirements for resilience, and the regulators encourage a community wide response in this space. CMORG can be expected to take a particular interest in this area, and rightly so.

In the meantime, also expect to be surprised as we see parts of our complex digital world fail in surprising ways which show just how interdependent our supplier ecosystem really is.