CharlesRussell Speechlys

Operational Resilience – Financial Services and Telecommunications

September 2019

Mark Bailey
Partner
T: +44 (0)20 7427 6519
mark.bailey@crsblaw.com

While cyber risk has taken much of the attention in the news, the UK government and regulators have been increasing their focus more generally on operational resilience and its impact on the economy.

The government monitors critical national infrastructure (CNI) closely, and both finance and telecommunications are regarded as CNI. The Cabinet Office publishes a public summary of Sector Security and Resilience Plans annually. The report notes that overall the finance sector has made good progress in improving resilience to threats, and indicated that future resilience exercises will be necessary, particularly in financial services:

> **Building Resilience**
> Over the next year, the Financial Authorities will deliver a comprehensive work programme to improve the resilience of the finance sector. We will ensure that we have the tools to deliver improved resilience, including drawing on the expertise of the National Cyber Security Centre and the Centre for the Protection of National Infrastructure.
>
> We will help the sector improve their operational resilience, including through exercises involving industry. We will also continue to improve our collective incident response capability and work closely with our international partners to develop our understanding of evolving threats to the global financial system.
>
> Source: Cabinet Office sector security and resilience plans (*page 16*)

As well as the recent focus on outsourcing, in particular the European Banking Association's (**EBA's**) final guidance on outsourcing agreements, there is a wider focus on concepts of business continuity and operational resilience. The Bank of England, Prudential Regulation Authority (**PRA**) and Financial Conduct Authority (**FCA**) accelerated the discussion more formally with its discussion paper (July 2018) "Building the UK Financial Sector's Operational Resilience".

This paper identified a concept of operational resilience to bring this to the attention of boards and senior executives in regulated firms. The paper concludes that vital elements of key business services are being delivered in the financial services sector by companies operating outside the regulatory perimeter, often concentrated among a few major providers. Increasingly this concentration risk includes the use of key cloud providers, including Amazon Web Services and Microsoft Azure amongst others. The report was followed by a paper from UK Finance and EY "operational risk in financial services" and a

second report from the CityUK and PWC "operational resilience in Financial Services – time to act", which this note looks at in more detail.

Both of the reports require a business to address its operational risk within the context of more developed security frameworks. Whilst these are in large part driven by cyber security, the concern over a national over-dependency on a small number of viable vendors is common also.

In the telecommunications sector, a recent report (July 2019) by the Department for Digital, Culture, Media and Sport (**DCMS**), the UK telecoms supply chain review report (CP158), addresses similar issues around concentration risk and how in the telecommunications sector's case concentration risk in the UK is principally focused on a handful of key vendors, particularly Ericsson, Huawei and Nokia, who supply the main UK mobile operators. News around Huawei's restricted listing in relation to communications equipment supply by the US government because of fears over technology risk has been clearly documented. In financial services, the debate has continued with a joint report from TheCityUK and PwC, "Operational resilience in financial services: time to act". This report draws on similar themes in a wider discussion on operational resilience.

What do these reports have in common?

The digitalisation of services means that the economy is more dependent on the services provided by third party and outsourced service providers, and their supply chains, and the impact of physical events such as power failures are also recognised as causing knock-on effects to digital services, where infrastructure business continuity measures fail.

Both reports also note the increasing importance of Cloud in the infrastructure ecosystem, in the case of telecommunications as necessary to deliver 5G, broadband rollout and "edge" services.

Both of the reports require a business to address its operational risk within the context of more developed security frameworks. Whilst these are in large part driven by cyber security, the concern over a national over-dependency on a small number of viable vendors is common also. This report looks at the themes in the reports around supply chain and how operators may have to address these in dealing with regulated organisations, whether in telecommunications or the financial services sector.

It is also interesting in the financial services area, to notice that the weight of regulation has so far fallen on banks and payments institutions, and that there is relatively little focus on insurance at this time. However, it must surely only be a matter of time before equivalent obligations are sought for insurance companies and their ecosystem.

The Cabinet Office report notes that sectors are totally interconnected: in particular it notes that the finance sector is not immune from threats to other CNI sectors, particularly energy and telecommunications. Regulated firms would be well advised to consider the impact of energy shortages or failure of energy to key suppliers such as data centres or critical facilities in this light, as well as more obvious telecommunications risk.

CharlesRussell Speechlys

The telecommunications industry is a key component of financial services and therefore the risks in this report should be reviewed in more detail by organisations reliant on telecommunications services. There is a clear risk that with regulators and governments so focused on this area that inconsistent policy making and recommendations could result, and therefore a deeper dive into these areas will be necessary for institutions seeking to manage risk and avoid regulatory inconsistency.

DCMS Report what does this address?

There is a clear risk that with regulators and governments so focused on this area that inconsistent policy making and recommendations could result and therefore a deeper dive into these areas will be necessary for institutions seeking to manage risk and avoid regulatory inconsistency.

The report notes that the most significant cyber threat comes from nation states in telecommunications. Further, supply chain risk is prevalent and the National Cyber Security Centre (**NCSC**) in the UK has identified a number of key security risks within the telecoms supply chain, in particular:

- national dependence on any one vendor, particularly those deemed high risk
- faults or vulnerabilities in network equipment
- "back door" risk, possibly permitting embedding of malign functionality in vendor equipment
- vendor administrative access to provide equipment support or as part of managed services contracts.

While a number of these are specific to the telecoms industry, these are common issues where IT equipment is deployed. In section 5 of the report the government announces that it will develop a security framework for 5G and full fibre networks with three key components:

- new Telecoms Security Requirements (**TSR**). These will be finalised with industry to ensure network design meets new security requirements in relation to their network security
- enhancing the legislative framework for security in telecommunications. Ofcom will be given stronger powers to enforce the new requirements and establish stronger national security backstop powers for government
- managing the security risks posed by suppliers. This will include the grading of suppliers according to risk. Careful note will need to be taken of this by institutions who may use any of these named suppliers so processes should be put in place in order to manage high risk vendors. It is also likely that these requirements will bring in an enhanced regulatory and perhaps contract framework that will need to be assessed by suppliers or by companies in the principal suppliers' subcontract chains.

Financial services: operational resilience

Following on from the joint PRA, FCA and Bank of England report, TheCityUK and PwC's and UK Finance and EY's reports both provide detailed recommendations for assessing, providing frameworks and governance for operational resilience and further guidance on supply chain. The provisions in

relation to how vendors will be further assessed, both in relation to concentration and operational resilience requirements, deserve careful reading by vendors and also an assessment by regulated institutions to review their operational and contractual requirements, particularly around "softer" requirements that may result from the report, including cooperation and collaboration and information supply arrangements, where consideration may need to be given to whether contracts should be enhanced so that the firm has the necessary information and controls for its own risk assessment.

… as a result of these regulations, issues such as step-in rights or the ability for institutions in more critical outsourcing contracts to "jump the chain" by taking over supervision of suppliers further down the supply chain, in the event of a principal supplier's failure, or mutual cooperation obligations between suppliers and supply chain, could start to become features that will have to be addressed in practice.

Possible matters for consideration arising from the CityUK report include enhanced contractual rights with regard to supply chain, and substitutability of suppliers or services in the event of service failure. Whilst not expressly stated in the report, the focus on common standards and collaboration both between institutions, and collaboration between suppliers to institutions, could mean that organisations are more likely to mandate cooperation between vendors, even on matters which would otherwise potentially be confidential, and the existence of vendor forums or information exchange requirements could start to become contractual features (albeit that confidentiality and competition law issues would have to be taken into account here). Further, as a result of these regulations, issues such as step-in rights or the ability for institutions in more critical outsourcing contracts to "jump the chain" by taking over supervision of suppliers further down the supply chain, in the event of a principal supplier's failure, or mutual cooperation obligations between suppliers and supply chain, could start to become features that will have to be addressed in practice. The effectiveness of remedies such as step in rights is rarely tested in practice, so firms should consider whether and how effective such measures are likely to be in the circumstances of material service agreements.

Further, the reporting obligations around transparency, giving information around a vendor's financial stability, and other events that potentially could change the financial position of the vendor, or reporting on concentration of risk of the vendor could become features that at least have to be considered in contracts.

Interestingly, the report cites cultural factors as being as important, if not more important, than contracts, but also states that perhaps new standard contract terms may be mandated, particularly where substitutability is limited. The focus on culture is a positive step as transparency between customer and supplier is essential, and this would support the strong efforts regulators have made in the finance industry to improve business culture. The suggestion regarding standard contractual wording is an approach that is increasingly being taken by the EU in business-to-business contracts with large scale or monopoly providers, so will deserve careful attention also. However, extensive contractual terms would be a controversial step by regulators as contracts and culture are closely linked. A contract can be used to drive supplier conduct, but the principal means for this is ensuring that the parties both have a common understanding of the goods and services to be provided and the governance mechanisms that moderate supplier behaviour. It is true that many larger organisations, in particular US-based cloud

and internet providers effectively regard their contracts as non-negotiable, particularly as regards liability, but they have adapted addenda for financial services and GDPR regulatory which at least partially address the regulatory requirements. If the regulators plan to adjust liability clauses or impact on the risk analysis of vendors, there will almost certainly be price adjustments. Any standard wording would also have to respect the extensive work that the technology and telecommunications industries have made to develop common standards and audit reports that are firmly based around operational processes, that should not be inconsistent with or overridden by contract provisions that could have unforeseen technical or cost consequences to implement.

Any standard wording would also have to respect the extensive work that the technology and telecommunications industries have made to develop common standards and audit reports…

In this context, the report expressly references ISO 22316/ 2017 in relation to information security. It is possible for organisations to mandate compliance with this standard as a contractual requirement, or to include the provision of necessary information by its suppliers to enable the firm itself to comply with the standard for its own business.

As a first step, firms need to analyse potential risks associated with suppliers, which may be exacerbated by concentration risk. It may be that firms are best served by bringing firms in, rather than keeping them at arm's length.

"*We require more from our vendors – we require them to be a partner more than a supplier*."

Interviewee

A sense of mutual resilience can be reinforced through common goals, with a shared mission likely to be as, or perhaps more, important than contracts and audit rights. Some firms have established joint operating committees for critical suppliers, which act as a clearing mechanism at CEO level and ensure there are no line management standoffs.

There is a question as to the role of regulators in respect of large, systemically important suppliers, some of which are bigger than their clients. In some senses, the financial services sector has become a net 'service taker'. Several of these monopoly/oligopoly providers, for example, in cloud services and data, are embedded in the infrastructure of the sector. However, currently there is a very real legal and regulatory lag in supply chains. There may be merit in regulatory guidance to drive new contract terms, particularly where substitutability is limited.

TheCityUK/PwC report, page 48

The report also records some potential risks from smaller suppliers who may provide niche or more traditional supplies.

The report also articulates a common concern amongst firms that it is not clear how far firms have to look down their suppliers' own supply chains in respect of risks. In a complex supply chains there may be three or more layers of subcontractors who form part of the solution. Of course, consistency with data protection is necessary in this regard where data protection provisions have to be flowed down through the supply chain in identical terms, although it is highly questionable how often this is in fact achieved. Further, the common requirement for firms to request veto or permission rights to changes in subcontractors may also be more honoured in the breach.

More data needed?

Operational resilience requires more data, both retrospective and prospective, and for this data to be provided according to a collaborative model.

Operational resilience requires more data, both retrospective and prospective, and for this data to be provided according to a collaborative model. In terms of management information, the report recommends that the optimum approach is forward looking and predictive information that incorporates near misses, echoing the FCA's focus in the area of conduct.

> A mindset of "attention to detail" (and not disregarding minor events) is likely to be productive in raising red flags and identifying potential threats to operational stability.
>
> TheCityUK/PwC report, page 30

This may be controversial in practice as suppliers may be very reluctant to provide this information on their own services but also the provision of information on this scale could potentially lead to a number of false positives that could in fact distract the business away from a real risk as and when it is starting to emerge.

Resilience by design – a way forward?

The report draws together much good practice and technical information, as well as regulatory analysis. It is by no means a set of concrete recommendations, but the frameworks suggested can provide working models for further development in the context of financial services, addressing the complex standards and regulatory environments should be aware of each other to avoid overlap and inconsistency. The concept of "resilience by design" echoes recent developments in data protection where privacy by design and privacy by default were a prominent feature of GDPR. It is not yet fully clear what this concept means in practice, or how it would overlap with the privacy by design and privacy by default principles of GDPR. The report notes that concepts such as this could require services to be ultimately built at scale, meaning that standardisation could in fact erode competitive advantage or lead to further consolidation in the industry.

Where the report is more helpful is potentially that the concept of substitutability can be applied to the third party relationships in the supply chain. This would require detailed review of business continuity plans, where firms could opt to retain a primary supplier but also to sustain backup relationships with secondary and tertiary suppliers to substitute in the event of the failure of the primary relationship. In practice this could be complex, requiring competitive suppliers to provide detailed confidential information about the nature of their services to ensure substitutability. This is a feature that in the US has proved controversial, given the high-level nature of many of the business continuity and recovery plans that the SEC noted in their own deliberations on similar topics.

A related strategy would be split providers across production and backup services so that firms can access backup data in the event of a disaster to recover more easily and then provide this data to alternative suppliers. A useful approach may be supplier symposiums to educate on regulatory requirements and need. The recommendations also recommend greater use of pooled audits, which in effect means maintenance by the suppliers of ISAE 3402 style certifications, or equivalent SOC 1 / SOC 2 reporting. This is an interesting contrast with the EBA guidelines where the EBA did not fully endorse use of such reports (*paragraph 92*). These reports are expensive to maintain for smaller suppliers, so there will be cost implications if these reports are universally required.

For systematically important providers, it is acknowledged that a "plan B" is unrealistic. As such, these organisations should potentially be invited to participate in stress testing exercises, and also potentially to bring these firms within the regulatory environment. This is approached obliquely and the report notes, "…regulators may also wish to consider reassessing the regulatory perimeter" (*page 48*). Ultimately, the operational resilience framework within the report could prove a useful model for further deliberation in light of the 20 recommendations made.

Conclusion

Given recent outsourcing guidance and other activity by government and regulators in relation to cyber security and operational resilience, there is a real concern that overlapping standards and guidance could create regulatory and operational friction, contrary to the express aims of improving security and operational resilience. A comparison between the approach in the telecommunications sector and the financial services sector indicates that regulators and government can take very different approaches according to the perceived security risks of the operators, and the uncertainty that cyber risk in particular presents. This note suggests a number of provisions for further consideration in relation to contractual risk, and perhaps how some of the softer, relationship-led factors could lead to a more constructive change in culture when compared with the more obvious concerns in the highly concentrated telecommunications industry.