A FINEXTRA WHITE PAPER
PRODUCED IN ASSOCIATION WITH IBM
JUNE 2016

HOW TO GET AHEAD ON OPERATIONAL RESILIENCE: STRATEGIES FOR FINANCIAL INSTITUTIONS

Finextra

01 INTRODUCTION

The importance of operational resilience in the financial industry has never been greater. The intensity of cyber-attacks targeting participants in the retail and commercial banking businesses as well as the financial markets is increasing all the time. In the context of cyber – and other less technically sophisticated but no less damaging types of internal and external fraud – maintaining security of critical data and systems is getting more and more difficult.

Meanwhile the regulators are levying severe fines on banks which suffer breaks in service that impact customers, and are constantly vigilant as to the systemic threat posed by the failure of major institutions or market infrastructures. In addition, the world's press is poised to expose and pillory any firm which suffers an operational break in this world of 'always on' services, especially one impacting information security. Social media savvy customers are vocal in following – and indeed often leading – the campaigns of humiliation. The reputational, financial and commercial damage caused by breaches of operational resilience in today's financial industry is severe.

Unfortunately, achieving operational resilience has never been harder. Whether motivated by politics or greed, the cyber-attackers are growing in number and marshalling an ever-more devastating armoury of weaponry – digital but also human in the form of rogue insiders – to carry out their assaults. Research suggests that around half of organisations doubt their preparedness to handle service disruptions as a result of cyber-attacks.

Financial institutions must also grapple with achieving resilience across increasingly complex architectures, with more integration and a growing number of critical systems. More organisational complexity is another challenge, and operational resilience must battle for resource and attention against many competing priorities. With retail and commercial banks under threat from disruption and digitally-driven new entrants, and suppressed returns on equity making life hard for investment banks, the money and focus required to meet operational resilience expectations must be difficult to come by.

Danièle Nouy, Chair of the ECB's Supervisory Board, acknowledged the challenging cost environment for banks during a speech in London earlier this year. "Cost-income ratios might not be the perfect metric, but for some banks in the euro area, high cost-income ratios indicate that there is some room for improvement in terms of efficiency," she commented. However she warned against achieving efficiency at the expense of resilience.

"Nevertheless, banks might also be tempted to cut costs where they should not. Inappropriate cost-cutting might, for instance, affect IT systems, putting their soundness at risk and exposing the banks to cybercrime or preventing them from coping with the challenges of digitalisation. The consequences could be operational losses, reputational damage and a disruption of business."

These threats to operational resilience are not theoretical. Some 40% of organisations in a study of more than 300 disaster recovery and business continuity professionals in North America, carried out by the IBM Center for Applied Insights, said they have had to execute their disaster recovery plans due to service disruptions during the past two years. And, as Nouy pointed out during her speech, not investing in operational resilience is categorically not an option. The natural activities of an organisation do not in themselves create resilient systems and processes, because there are too many conflicting pressures. Therefore a conscious effort must be made to put resilience in place, combining preparation (proactive measures to avoid and/or speed recovery from incidents: it is always cheaper to solve resilience issues in advance at the design stage) and demonstration (events that prove the success of the preparation).

> "For some banks in the euro area, high cost-income ratios indicate that there is some room for improvement in terms of efficiency. Nevertheless, banks might also be tempted to cut costs where they should not. Inappropriate cost-cutting might, for instance, affect IT systems, putting their soundness at risk and exposing the banks to cybercrime or preventing them from coping with the challenges of digitalisation. The consequences could be operational losses, reputational damage and a disruption of business"
>
> DANIÈLE NOUY, CHAIR OF THE ECB'S SUPERVISORY BOARD

But is it possible to transform operational resilience from an area in which financial institutions grudgingly invest as a damage limitation measure, to an activity which banks perceive as an opportunity to take a leading and differentiating role?

This paper will argue that it is. Financial institutions which acknowledge that to succeed they must invest in preparation, expect failure and invest in recovery – accepting that while preventative measures will work much of the time, disruptions are nevertheless inevitable and have a lifecycle that can be managed to their benefit if a proactive approach is taken – do have a chance to get ahead in operational resilience. In turn, they will potentially find new regulation in this area easier to comply with, and they will certainly be resuming revenue generating activities more rapidly than competitors with a laggardly attitude to operational resilience. Firms tackling this challenge head-on will also have a better story to tell customers and the media when the inevitable happens, which could help mitigate the fallout in terms of reputational damage.

Examining drivers for improving operational resilience, impediments to doing so, possible approaches to deploy and their benefits, the paper will also provide practical insights into how to transform this activity from challenge to opportunity – as well as emphasising that there is no time to lose in forging ahead in the operational resilience race.

> “Financial institutions which acknowledge that to succeed they must invest in preparation, expect failure and invest in recovery, do have a chance to get ahead in operational resilience.”

02 WHY IS OPERATIONAL RESILIENCE SO CRITICAL – AND SO DIFFICULT TO ACHIEVE?

If operational resilience is defined as the ability to rapidly adapt and respond to dynamic changes – opportunities, demands, disruptions, threats – with limited impact to the business, and with a scope that spans people, process and IT, then it is pretty clear that most financial institutions' operational resilience muscles will be getting a significant workout in this time of constant change. Regulation, technology, customer requirements, the occasional curve-ball like Brexit, all contribute to creating a potentially highly destabilising environment for firms without the right operational resilience mentality.

The cyber threat

It almost goes without saying that cyber-threats and the pressure to maintain data and system security are a major reason for the current preoccupation of the financial industry and its regulators with operational resilience. Think Bank of Bangladesh and Vietnam's Tien Phong Bank – and how much better it sounded for the latter to be able to say it had foiled an assault by cyber-attackers using fraudulent SWIFT messages, unlike the former, which had to admit to losses of EUR81m. Think denial of service attacks, malware, ransomware... According to Kaspersky Lab's Q1 2016 malware report, the company's experts detected 2900 new malware modifications during the quarter, an increase of 14% on the previous quarter. Kaspersky Lab's database now includes about 15,000 ransomware modifications, and the number continues to grow. In the first quarter of 2016, Kaspersky Lab security solutions prevented 376,602 ransomware attacks on users, 17% of which targeted the corporate sector.

Other data sources also paint a grim picture of cyber-threats in recent times. IBM X-Force monitors the latest threats – including vulnerabilities, exploits and active attacks, viruses and other malware, spam, phishing, and malicious web content – in order to advise the general public on how to respond to emerging threats and to deliver security content, products and services to help protect IBM customers.

By January 2016, IBM X-Force had tracked 272 security incidents for 2015, on par with the 279 incidents tracked in 2014. In terms of total disclosed records, 2014 was notable for more than one billion records being leaked, while 2015 was down to a still staggering 600 million leaked records in incidents tracked by X-Force using public breach disclosures. The IBM X-Force findings for 2015 show that IBM's average client company experienced 178 security incidents in 2015, up 66% from the 109 that took place in 2014. This equates to roughly 3.4 incidents per week – up from 2 per week in 2014.

The IBM X-Force data also shows that the number of breaches in the financial services industry that involved extortion tactics or theft of currency rose considerably – by 80% – in 2015. As for technical methods, together the attacks related to malicious attachments or links and Shellshock (the family of security bugs in the widely used Unix Bash shell) made up nearly 38% of those targeting financial institutions in 2015. In short, the cyber-attack spectres are legion and growing.

The estimated annual cost of global cyber-crime is $100 billion – equating to 556m victims per year, 18 per second. Some predictions suggest cybercrime will become a $2.1 trillion problem by 2019. According to the 2015 Cost of Data Breach Study by IBM and the Ponemon Institute, the average total cost of a data breach increased from $3.52 million in 2014 to $3.79 million. Financial institutions are high on the list of targets as the criminals follow the money. The response is an increasing investment in sophisticated security measures to combat the cyber attackers. By 2017, the global cyber-security market is predicted to amount to $120.1 billion, compared to $63 billion in 2011. But the security will not always work, and in the IBM Center for Applied Insights research "addressing cyber-security risks" was identified as a top resiliency challenge by 49% of respondents.

> "The IBM X-Force findings for 2015 show that IBM's average client company experienced 178 security incidents in 2015, up 66% from the 109 that took place in 2014. This equates to roughly 3-4 incidents per week."

Complexity and interconnectedness

Interestingly, 55% put “including an increasing number of critical systems in disaster recovery plans” among their top challenges – with 48% opting for “managing more points of disruption due to greater integration”. The challenge of IT complexity is a major one. On top of issues with legacy infrastructure which is inflexible and hard to fix, financial institutions are adding ever more layers to manage. The rise in use of cloud solutions and other outsourcing options is a factor here – a particular issue if cost reduction goals have won out over service quality – as are digital front ends and mobile apps in the retail and corporate banking space and low latency and co-location in the financial markets arena.

Most organisations seek to drive change in line with their strategic goals and undertake projects which can add significant new capability, or rework and replace major parts of the organisation. While change control is often a feature of major projects, they can sacrifice functionality or quality for time to market, often struggle to integrate with the rest of the organisation and inadequately prepare for the future BAU operation of these new systems. In addition, a lot of change occurs on a small scale, through incremental additions or alterations. These changes can often attract less oversight and control than major projects.

The interconnectedness of financial technology infrastructure today is also a concern. Think RBS and its £56m fine following the 2012 outage – delivered along with a major slap on the wrist for the widespread nature of the impact (caused by a routine software upgrade going wrong), across many customer-facing activities, and lasting many weeks – attributed by the regulator to “a very poor legacy of IT resilience and inadequate management of IT risks”.

When everything depends on technology, nothing works when the technology fails – and that is bad news in the ‘always on’ world.

> “The challenge of IT complexity is a major one. On top of issues with legacy infrastructure which is inflexible and hard to fix anyway, financial institutions are adding ever more layers to manage. The rise in use of cloud solutions and other outsourcing options is a factor here – a particular issue if cost reduction goals have won out over service quality.”

Regulatory pressure

At an industry level this interconnectedness and high degree of technology dependence is a concern for the regulators looking to identify and eliminate sources of systemic risk. We have already seen IOSCO's principles for resilience for systemically important market infrastructures, and all the indications are that going forward the supervisors will be increasing attention to operational resilience. They will focus on risk identification and mitigation, contingency planning, stress testing and market-wide exercises (such as the Resilient Shield exercise in the UK) to assess the resilience of individual firms and the system as a whole.

Ironically though, some of the new regulation coming in will increase operational resilience challenges for financial institutions. Think of the data protection issues that could be created for account owning institutions (banks) under PSD2, as they are forced by regulation to make customers' transaction information available to new payment services players. Think of reporting entities under MiFID II having to file transaction reports on a vastly increased number of asset types and using a much bigger number of fields – and being exposed to the risk of illegally sharing sensitive customer information.

Disruptive technology

If regulation is a double-edged sword in the battle to achieve operational resilience, then so are some of the new technologies which on the face of it promise so much for the future efficiency and effectiveness of the financial markets. Take blockchain. In theory, distributed ledger-based systems should be more resilient to systematic operational risk because the system as a whole is not dependent on a centralised third party. A distributed system effectively has as many redundant back-ups as there are contributors to the network. The ledger exists in multiple copies which should make it more resilient than a centralised database. And historic transactions are unalterable and permanently accessible to all authorised participants, ensuring that if an attack does occur each participant's balance is traceable.

All true no doubt. However, as Andrew Hauser, Executive Director for Banking, Payments and Financial Resilience at the Bank of England put it when he spoke at a recent London conference, when it comes to blockchain, "what begins as a discussion about technology quickly comes back to a question about what this technology does to the distribution of risk". Even Blythe Masters, CEO of blockchain leader Digital Asset Holdings, speaking at the same conference, acknowledged the challenge in transitioning from today's environment to the blockchain future. "Why isn't it happening more quickly? It's difficult. Legacy systems are gigantic. They are processing trillions of dollars notional daily, and if they fail it's catastrophic," she said. "This will be like changing the wheels on a bus on a fast-moving highway." One analyst listening to these discussions was prompted to tweet, "Whose head is going to be on the block for project risk of moving from 30+ years' mainframe to blockchain tech?"

Indeed, it can seem like cutting edge technology gives with one hand but takes away with the other. According to IBM's 2015 Cyber Security Intelligence Index, companies experienced an average of 81 million security events in 2014. Identifying false positives is getting more difficult as the amount of data to process, turn into insights, and use to make decisions proliferates. IBM predicts that cognitive computing will become a security assistant to help security professionals and data analysts cut down the noise and focus on the real threats and benefits to their organisations. But IBM also predicts that when it comes to another much-vaunted technology development – the Internet of Things (IoT) – there will be an increase in 'non-traditional' attack targets, in addition to incidents of cars, TVs, baby monitors and gaming platforms being compromised.

In response, predicts Gartner in its latest pronouncements on IoT, worldwide spending on IoT security will reach $348 million in 2016, a 23.7 percent increase from 2015 spending of $281.5 million. Spending on IoT security is expected to reach $547 million in 2018. Worryingly, Gartner predicts that by 2020, more than 25% of identified attacks in enterprises will involve IoT, although IoT will account for less than 10% of IT security budgets.

In short, technology complexity and interconnectedness are creating an operational resilience headache today, and this is likely to continue into the future – especially as experience suggests that new layers of technology rarely eliminate earlier ones, rather they add further to the stack.

> "Why isn't [the transition to blockchain] happening more quickly? It's difficult. Legacy systems are gigantic. They are processing trillions of dollars notional daily, and if they fail it's catastrophic. This will be like changing the wheels on a bus on a fast-moving highway."
>
> **BLYTHE MASTERS, CEO, DIGITAL ASSET HOLDINGS**

The people part

People – individually and collectively – represent an important dimension of the operational resilience challenge. People make mistakes, and these inevitable human errors can go unnoticed at the time. In addition, complexity and fragmentation are not the sole preserve of technology. They manifest equally strongly in banks' organisational structures and workforces today – whether as a result of mergers and acquisitions or outsourcing to third-parties. Achieving common understanding of and buy-in to an operational resilience culture across a globalised workforce is no mean feat, especially in the context of an acknowledged reduction in the number of experienced operational resilience professionals available.

The culture of an organisation has to support its operational resilience goals. A decision must be made as to how an institution's brand values will impact these goals – Volvo or Ferrari? – and this must sensibly consider context and display situational awareness. The most thoroughgoing operational resilience approaches should be matched with the biggest areas of risk and the biggest areas of impact should an incident occur. Once the approach has been settled upon, the culture must support it, and banks must find ways to motivate their workforces to view operational resilience as a positive driver of effort – not a necessary but painful and regrettable insurance premium. A critical element is senior management involvement in operational resilience planning. The stakes are high. Investments in resilience must align with organisations' most critical business needs.

> "Complexity and fragmentation are not the sole preserve of technology. They manifest equally strongly in banks' organisational structures and workforces today – whether as a result of mergers and acquisitions or outsourcing to third-parties."

03

WHAT OPTIONS DO BANKS HAVE TO GET AHEAD IN OPERATIONAL RESILIENCE?

Focus on industry collaboration

Collaboration between firms and regulators is as critical as internal collaboration within a firm. There are industry initiatives under way already to share security oriented data, events, processes and best practices. For example, the Financial Services Information Sharing and Analysis Center (FS-ISAC) is a member-driven, non-profit organisation working to ensure the resilience and continuity of the global financial services infrastructure. Furthermore, Soltra – a company operated by FS-ISAC and DTCC – has as its stated mission to design and deliver solutions that increase resiliency to cyber and physical risks and threats for critical sector entities worldwide. Soltra's flagship tool distils massive amounts of threat intelligence – taking threat intelligence from any source, in any format, de-duplicating it, automating sightings and prioritising actions, routes intelligence to users, devices and communities in real-time and reduces the threat indicator analysis lifecycle.

However, there is scope to take this further, for example with industry-wide testing and simulation exercises that go beyond security and cyber-security scenarios. Building on the Basel II Operational Risk initiatives, such as the Operational Risk Exchange (ORX), more can be done to consider and share best practices, especially around testing, architectures and engineering practices, as well as all aspects of service management practices.

> "Collaboration between firms and regulators is as critical as internal collaboration within a firm. There are industry initiatives under way already — and there is scope to take this further."

Focus on assessments and annual audits

Preparation and practice should be priorities, in order to increase ‘operational muscle memory’. One approach is to build on the three lines of defence model (operational management, risk management and compliance functions, internal audit) and obtain an external neutral view of the operating environment through a thorough assessment of the current landscape. This should not be just a ‘tickbox’ exercise, but rather the opportunity for a collaborative learning experience, challenging the status quo and planning for a better future state. There is pressure for more Board accountability and to grow IT expertise on the Board, which can be a factor in the assessment and forward planning. Financial institutions could look to partners with tried and tested resilience frameworks, methods and approaches which have been used by banks and exchanges globally to help determine focus and produce a repeatable approach to assessments. There are methodologies out there which span strategy, architecture, organisation, processes, governance, applications, data and IT and data centres. Over time these assessments can evolve to become an annual process to check ongoing progress and remind organisations to continuously prioritise operational resilience.

Focus on service thinking

Another approach is to break down the organisation into discrete component services, comprising all aspects of business, technical and operational competencies. This enforces a clear separation of concerns and clarifies who is responsible and who is ultimately accountable. Equally important is then to consider the interactions and dependencies between the services – producing clear contracts for each interaction.

For each service and each service contract as much data needs to be collected as possible to help understanding of the environment – for example, gathering the discrete costs of the service and documenting data flows, process flows, security elements, non-functional requirements and reporting requirements. All this information can be collected and maintained in a service portfolio management system. This approach can be summed up by the “If you can’t measure it, you can’t improve it” mantra. The clarity of insight gained from such an approach will help inform operational resilience initiatives.

Focus on taking a proactive approach to resilience engineering

Resilience is a combination of preparation and demonstration, where preparation puts in place proactive measures to avoid incidents and/or speed recovery from them, while demonstration comes from the events that prove the success of that preparation. Planning is essential to establishing your services on a secure footing and, as always, it is cheaper to solve resilience issues in advance at the design stage. When a capability is deployed, it needs to be checked and tested to ensure it is effective. This checking may be a planned test, or it may be observing your capability in action as it limits or avoids service impact.

Financial institutions should consider resilience engineering methods which take into account resilience design, prevention, validation, action and assurance. Such methods encourage taking a proactive approach to addressing the full lifecycle – from analysis, design, build, test and transition to production, system maintenance, availability management and knowledge management.

> "Resilience is a combination of preparation and demonstration. Planning is essential to establish your services on a secure footing and, as always, it is cheaper to solve resilience issues in advance at the design stage."

04

WHAT DO LEADERS IN OPERATIONAL RESILIENCE STAND TO GAIN?

Banks which face the challenges outlined in this paper head-on and achieve a high level of operational resilience based on an integrated, flexible approach and frequent, robust testing, stand to gain in a number of ways, including:

- Achieving recovery time objectives, ensuring rapid resumption of interfaces with partners and the ability to ensure rapid resumption of revenue-generating processes;
- Reducing recovery costs; and
- Being able to report their business recovery performance is better than others in their industry.

In short, achieving market leading operational resilience enables banks to turn the three areas in which operational resilience failures can cause significant damage – commercial, financial and reputational – into areas of positive differentiation.

05

CONCLUSION

This paper has established that given the growing demand for 24/7 'always on' services and an increasingly stringent regulatory approach to operational failures, the importance of operational resilience in the financial industry is greater than ever.

It is also clear that an operational resilience strategy based on a structured assessment – driven by a conscious, deliberate and proactive approach to preparation and demonstration – enables banks to achieve and prove higher levels of resilience. This is important to gain the confidence of customers and regulators. It is also an essential underpinning for the successful achievement of business goals in today's ever-changing environment.

06 ABOUT

Finextra

This report is published by Finextra Research.

Finextra Research is the world's leading specialist financial technology (fintech) news and information source. Finextra offers over 100,000 fintech news, features and TV content items to visitors to www.finextra.com.

Founded in 1999, Finextra Research covers all aspects of financial technology innovation and operation involving banks, institutions and vendor organisations within the wholesale and retail banking, payments and cards sectors worldwide.

Finextra's unique global community consists of over 30,000 fintech professionals working inside banks and financial institutions, specialist fintech application and service providers, consulting organisations and mainstream technology providers. The Finextra community actively participate in posting their opinions and comments on the evolution of fintech. In addition, they contribute information and data to Finextra surveys and reports.

For more information:
Visit www.finextra.com, follow @finextra,
contact contact@finextra.com
or call +44 (0)20 3100 3670

IBM United Kingdom

IBM is a globally integrated enterprise operating in over 170 countries. Today IBM UK has around 20,000 employees, bringing innovative solutions to a diverse client base to help solve some of their toughest business challenges. In addition to being the world's largest IT and consulting services company, IBM is a global business and technology leader, innovating in research and development to shape the future of society at large. IBM's prized research, development and technical talent around the world partner with governments, corporations, thinkers and doers on ground breaking real world problems to help make the world work better.

For more information:
Visit ibm.com/industries/uk/en/banking

Finextra Research Ltd
101 St Martin's Lane
London
WC2N 4AZ
United Kingdom

Telephone
+44 (0)20 3100 3670

Email
contact@finextra.com

Web
www.finextra.com