Managing Risk, Leveraging Technology and Building Resilience for the World's Official Institutions

A Conversation on Cyber Security and Operational Resilience

ORC
Operational Risk Consulting Limited

STATE STREET.

As data continues to grow in importance, official institutions today face increased complexity in operating models and require heightened diligence.

In this white paper series, State Street partners with Operational Risk Consulting to explore these challenges and engage in a discourse to navigate them.

Navigating through Cyber Security for Operational Resilience

Loss of access to data and analytics, interruptions to the ability to execute trades, and breakdown in communications with clients, partners or service providers can be catastrophic for any organization.

Operational resilience took center stage in the industry as the pandemic unfolded in 2020 and businesses were focusing on adapting to the challenges around continuity, connectivity and communications.

While it became imperative to have a strong operational infrastructure, the risks to operations were also a matter of concern for organizations. Cyber security topped the list as companies moved from working from office to remote working. This challenge will spill over in the post-pandemic world as the conventional ways of operating have now transformed with distributed working being the new normal for many official institutions.

However, this opens new avenues of risk in terms of secure communications, data sharing and systems interoperability. These challenges pose institutions with several questions, beginning with how can they build and organize their systems to be more resilient.

In an interconnected and interdependent world, building resilience into an operating model is not just an internal challenge. Investment operations are an ecosystem of ongoing strategic relationships with third-party providers including technology, data, analytics or client services.

Our head of EMEA Insights, James Redgrave speaks to Dan Money, our head of Operational Resiliency in EMEA, Neill Newman, our head of Information Security in EMEA and Nigel Morriss, chief executive officer of Operational Risk Consulting, about how investment institutions, especially official institutions, need to understand that addressing resilience in all its complexity is the need of the hour.

A Conversation on Cyber Security and Operational Resilience

Dan Money
Head of Operational Resiliency,
EMEA, State Street

Neill Newman
Head of Information Security,
EMEA, State Street

Nigel Morriss
Chief Executive Officer,
Operational Risk Consulting

James Redgrave
Moderator, Head of EMEA
Insights, State Street

Resilience Best Practices

James: I'd like to talk about resilience and best practices for setting up a resilient set of operations. What to do at the very beginning to make the best possible start, in operational resilience with a particular focus on technology and cyber?

Dan: The first key element of resilience is identifying your critical business services. That can be areas that hit market stability or firm viability or the consumers. The second aspect is to map that end-to-end and identify what your key dependencies are. What are you dependent on to deliver those services? Third, you can then set metrics or tolerances in terms of disruption to those services. Fourth, you need to develop some way to measure them in real time and assess any forward-looking impacts that are coming up. The fifth element is to test it, either through scenarios or through looking at incidents that you've seen.

Neill: From a cyber perspective, Dan mentioned understanding what your critical services are and that means understanding the people and process elements – the technology element is not just about technology. Forgetting people or process and their resiliency can be a detriment if you are trying to recover in a certain situation. The other piece is about how you recover. It's also important to have an understanding of what you would do when it goes wrong and how you respond to recover those services back to deliver to the clients or to the regulators.

Nigel: You also need to think about robustness. When we talk about robustness, we mean how models need to be built and whether you've got something that's been carefully designed and implemented with resilience in mind. When there is an event and resilience is required, you can bounce back – ensuring you bounce in the right direction. We have to go back to the basics and just like building a house, the foundations need to be strong. Also, all other elements of the build, which are integral to the overall integrity of the structure, are critical. I think the Basel Banking Commission gave the simplest definition of operational risk. It's fundamentally building to protect against the risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. It really does cover such a vast area of considerations.

Dan: It's a great point about the robustness and the foundational elements. Are we set up in the right way? Or have we built things piecemeal when we needed to look at it end-to-end, holistically and from an efficiency perspective? I think sometimes people look at how we need to do it from a regulatory perspective, but we also need a best practice perspective. It's also going to give you some good business outcomes from putting that lens on it.

Neill: Yes, this isn't a one-time exercise, it's continuous. While you can design, plan and be ready for certain events, there are other things that are happening inside an organization. Organizational change, structural changes, business strategy changes that lead to changes in your resilience. So, while you can design something at the start that is resilient, over time the natural changes in an organization can make those systems less resilient.

Nigel: There is no one-size-fits-all. There are some gold standards but what one has to do with a best practice standard is take it in the relevant circumstances to which it needs to be applied. As long as there's no compromise to the black and white rules, it needs to be applied specifically to the task at hand – to the financial institution, to the client, to the investor that you're working with and to the jurisdiction that they're in. With operating models and their robustness, there's nothing that should be static. Technology changes at a rapid pace. Data systems change. Regulation has taken on an entirely new meaning in everybody's lives. As an example, a few years ago many board members wouldn't have known the real implications of cyber security. Now this is a board-level discussion where risk management and many areas of business must be involved to ensure appropriate ongoing resiliency. Perhaps that's because the threats to organizations – financial and non-financial – have grown to where there are not just criminal enterprises but state actors.

Monitoring Resilience and Recovery

James: I want to move on to this idea of an ongoing process. Once you have your best practice standards in place, you have to ensure that you maintain them. What are the best ways of doing this?

Neill: From a cyber perspective, it's about understanding what you have and spending time looking into those processes. Have you got a continuous measurement and how well is it doing? It may be that a particular service line is more important than another one. So how do you get visibility and how do you measure to make sure that you're delivering what is expected by the customers, in some cases regulators, and ultimately for the value of the shareholders? How do you ensure continuous improvement – updating the organizational changes or threats that you face in each one of those areas.

The other element to overlay onto that is governance. It's all well and good asking the IT guys, "Are the systems okay?" They say, "Yes, they're all good." But how are you overseeing that? How are you challenging that? How do you know you're getting the correct information? So, there's a process of validation and challenge that is also required.

Nigel: Go deep is what I would say. I understand the risk landscape that an organization may be exposed to and how it can manage that risk. We have to understand that risk is inherent. It's there in the financial organizations that we work and deal with. So, to be able to truly identify the risk landscape and manage it on an ongoing basis, you have to go end-to-end across the organization and beyond, depending on third parties. We look at investment structures or those frameworks that are in place to support investment structures: custody; compliance frameworks; risk management; audit functions; investment controls or investment support controls that support the lifecycle of assets and asset administration; data continuity frameworks; and then third-party management.

James: What does an organization need to have in place in terms of recovery when something happens that really puts pressure on their operations and systems, to the point of failure?

Neill: There are many things that will be thrown at you that you have not considered for whatever reason, whether that's through lack of planning or an abnormal event that nobody has considered before. In those situations, what you need is clear communications with the right people and they can vary. It obviously will include senior management, but it could include your legal teams, external communications teams, IT, or business operations. It's choosing the right people at the right time to bring into those conversations. The second thing is not panicking and logically understanding what has happened. In that information void during a particular event, you can actually make what seemed to be good decisions but turn out to be drastically bad decisions. Then, of course, after the event, learning from it.

Nigel: We've talked about things going wrong, but I always like to call out the near misses too. In the operational risk management frameworks that Dan has mentioned a near miss is often the same as an actual error or loss event – you're just lucky that it didn't transpire. We have to treat it the same because there was a control failure. Therefore, we promote straight-through processing automation. We get very nervous when things slide out into the manual realm. But when they do, you need a framework of appropriate signatories signing off something that can be supported consistently in an error-free way. The right controls and ongoing oversight must be put in place to support that. Plan it with the people in mind because it's people who are chosen specifically based on their deep experience and their knowledge.

Dan: The other thing that we focus on in incident management is to try keeping things to a standard and try not to do too many ad hoc things, because that's when you're introducing risk. Try and maintain standard processing, standard procedures, standard controls as far as possible so that you're not introducing new risk into what is already probably an out of the ordinary incident.

Technology Enhancing Resilience

James: We've talked about the potential for risk that cyber introduces into the resilience sphere. I'd like to talk a little bit about how technology can create opportunities to generate better resilience and due diligence. Both internally and in terms of your external relationships, how can technology better promote the practices we've been discussing?

Neill: One area that is incredibly important as you get into the technology space is standardization. If you have a technology footprint or an operational footprint that is complex, that is messy, that is non-standard, then quite clearly, the complexity of that will lead to more failures and therefore a less resilient system. So, understanding what you have, simplicity and standardization are the ultimate aims. It's difficult to achieve that, but the more you can do to standardize your technology and your operations, the easier it is to understand when something is wrong.

Dan: We have built a tool that helps us with process mapping and looking to link together taxonomies because all the information is already there, but can you identify the key repositories of your dependencies or third parties, people or locations? If you can use technology to link those together and allow you to analyze them from an ongoing vulnerability point of view, then that can be a very powerful tool.

Neill: It also helps bridge the gap between what has culturally and historically been the divide between business operations and technology. Business operations understand the business process. The technologists understand the nuts and bolts. But it's where they interface and what the implications are for each other, that it can become blurred. If you have that end-to-end process map for operations – the systems that they're operating on, the technologies that they're operating on, the physical location of those pieces of infrastructure, the servers, the networks, firewalls, etc. You can then truly understand the risk that you are managing and that's the ultimate goal.

Nigel: There's a growing theme here of regulatory concern around organizations understanding the risk that their third parties are exposed to and information technology risk. I think we'll begin to see growing momentum from the regulators in ensuring that we look at the technology space, because it does promote resiliency. You can't afford to have interruption to business as usual. You need those prices. You need those data feeds. You need that cleaning and cleansing tool facility. You need to be able to aggregate that data. I think technology can and does provide opportunities and it does promote resiliency, but it all goes back to understanding. Do you truly have a clear line of sight into what the underlying processes and controls are that your third parties have?

Neill: That kind of assessment comes back to how risk averse you are in your diligence. If you go that extra step, your third parties typically rely on another third party; a fourth party. Do you go the extra mile with the fourth party and if that fourth party is relying on a fifth party, and so on? You can quite clearly see the sprawl that would create and the complexity that is probably too difficult a problem for any one organization to objectively measure. There's a level of pragmatism that has to be taken into account because, while in an ideal world you would understand everything, the practicalities mean that you can't. It's about understanding where that line is and making the right decision.

Third Parties and Due Diligence

James: That brings us on to third parties. Presumably, you need an ability to do due diligence on your third parties' due diligence. You obviously can't check all their suppliers and providers, but you can check the systems that they have in place to check them. It's like a hall of mirrors, from one position you can see all the way down.

Dan: Exactly. Your due diligence on them – a key aspect of it – is how do they conduct due diligence over their key suppliers? Have they identified their key suppliers? What checks are they doing over that chain of outsourcing elements that you invariably see in operating models today?

Neill: You can split operational risk of resilience into two camps. One is the areas where the variables are controllable. For example, with an interest rate fluctuation, you know what the interest rate is going to vary between two fixed things whether that's zero to negative, whether it's positive, depending on what the economic circumstances are. But it's a very – I hesitate to use the word simple – but it's a controlled situation where the variables are minimal. If you then move into a lot of IT risk the number of variables involved are significant and sometimes almost impossible to quantify. Therefore, in the first situation where you've got a bounded problem, you can usually get to a robust answer within a degree of accuracy. When you get to some elements of cyber security and IT security and operations, the variables are so vast, it's very difficult to actually pinpoint that, 'This is the risk.' You can measure the impact of a cyber event, for example. But calculating the likelihood of those situations occurring is difficult. So those organizations that treat cyber risk as something we are absolutely able to quantify 100 percent in order to make decisions on resiliency and so forth start to fall apart when you start talking about the likelihood of these events occurring. I think there's an evolution or a maturity that needs to occur that understands and respects the complexity. It is not an excuse; it's just the nature of the problems are different in the cyber world.

Dan: Certainly, the view of some of regulators is they're now saying they want you to assume failure of key dependencies and then analyze what that would mean to you. I think that it's a move from the likelihood question to, 'Things will go wrong and often beyond your control.' If they go wrong, how will you deal with that? In our scenario testing that we're doing now, we stopped trying to build scenarios. We just say this has failed. It's failed for these many days. How would you deal with that? It takes that likelihood element away from it in terms of your testing of your key dependencies.

"I think there's an evolution or a maturity that needs to occur that understands and respects the complexity. It is not an excuse; it's just the nature of the problems are different in the cyber world."

— NEILL NEWMAN

About State Street

State Street Corporation is one of the world's leading providers of financial services to institutional investors including investment servicing, investment management and investment research and trading. State Street partners with official institutions, sovereign wealth funds, central banks and other official institutions globally to help address their biggest challenges.

About Operational Risk Consulting

Operational Risk Consulting or 'ORC' is a UK-based specialist risk management advisory firm, which advises institutional asset owners on managing the operational risks associated with investing. ORC's key objective is to help raise investment operations standards.

For more information, visit:

statestreet.com/ideas

STATE STREET.

State Street Corporation
One Lincoln Street, Boston, MA 02111

www.statestreet.com

Disclaimer

The material presented herein is for informational purposes only. The views expressed herein are subject to change based on market and other conditions and factors. The opinions expressed herein reflect general perspectives and information and are not tailored to specific requirements, circumstances and/or investment philosophies. The information presented herein does not take into account any particular investment objectives, strategies, tax status or investment horizon. It does not constitute investment research or investment, legal, or tax advice and it should not be relied on as such. It should not be considered an offer or solicitation to buy or sell any product, service, investment, security or financial instrument or to pursue any trading or investment strategy. It does not constitute any binding contractual arrangement or commitment of any kind. State Street is not, by virtue of providing the material presented herein or otherwise, undertaking to manage money or act as your fiduciary.

You acknowledge and agree that the material presented herein is not intended to and does not, and shall not, serve as the primary basis for any investment decisions. You should evaluate and assess this material independently in light of those circumstances. We encourage you to consult your tax or financial advisor.

All material, including information from or attributed to State Street, has been obtained from sources believed to be reliable, but its accuracy is not guaranteed and State Street does not assume any responsibility for its accuracy, efficacy or use. Any information provided herein and obtained by State Street from third parties has not been reviewed for accuracy. In addition, forecasts, projections, or other forward-looking statements or information, whether by State Street or third parties, are not guarantees of future results or future performance, are inherently uncertain, are based on assumptions that, at the time, are difficult to predict, and involve a number of risks and uncertainties. Actual outcomes and results may differ materially from what is expressed herein. The information presented herein may or may not produce results beneficial to you. State Street does not undertake and is under no obligation to update or keep current the information or opinions contained in this communication.

To the fullest extent permitted by law, this information is provided "as-is" at your sole risk and neither State Street nor any of its affiliates or third party providers makes any guarantee, representation, or warranty of any kind regarding such information, including, without limitation, any representation that any investment, security or other property is suitable for you or for others or that any materials presented herein will achieve the results intended. State Street and its affiliates and third party providers disclaim any warranty and all liability, whether arising in contract, tort or otherwise, for any losses, liabilities, damages, expenses or costs, either direct, indirect, consequential, special or punitive, arising from or in connection with your access to and/or use of the information herein. Neither State Street nor any of its affiliates or third party providers shall have any liability, monetary or otherwise, to you or any other person or entity in the event the information presented herein produces incorrect, invalid or detrimental results.

No permission is granted to reprint, sell, copy, distribute, or modify any material herein, in any form or by any means without the prior written consent of
State Street.

3672900.1.1.GBL.INST Expiration date: 8/31/2022