THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

OPERATIONS

Collaborating for the greater good: Enhancing operational resilience within the Canadian financial sector

FILIPE DINIS | INDERPAL BAL

20
YEAR ANNIVERSARY

OPERATIONAL RESILIENCE

#53 MAY 2021

THE CAPCO INSTITUTE

JOURNAL OF FINANCIAL TRANSFORMATION

RECIPIENT OF THE APEX AWARD FOR PUBLICATION EXCELLENCE

CONTENTS

OPERATIONS

TECHNOLOGY

MILITARY

DEAR READER,

Welcome to this landmark 20th anniversary edition of the Capco Institute Journal of Financial Transformation.

Launched in 2001, the Journal has followed and supported the transformative journey of the financial services industry over the first 20 years of this millennium – years that have seen significant and progressive shifts in the global economy, ecosystem, consumer behavior and society as a whole.

True to its mission of advancing the field of applied finance, the Journal has featured papers from over 25 Nobel Laureates and over 500 senior financial executives, regulators and distinguished academics, providing insight and thought leadership around a wealth of topics affecting financial services organizations.

I am hugely proud to celebrate this 20th anniversary with the 53rd edition of this Journal, focused on 'Operational Resilience'.

There has never been a more relevant time to focus on the theme of resilience which has become an organizational and regulatory priority. No organization has been left untouched by the events of the past couple of years including the global pandemic. We have seen that operational resilience needs to consider issues far beyond traditional business continuity planning and disaster recovery.

Also, the increasing pace of digitalization, the complexity and interconnectedness of the financial services industry, and the sophistication of cybercrime have made operational disruption more likely and the potential consequences more severe.

The papers in this edition highlight the importance of this topic and include lessons from the military, as well as technology perspectives. As ever, you can expect the highest caliber of research and practical guidance from our distinguished contributors. I hope that these contributions will catalyze your own thinking around how to build the resilience needed to operate in these challenging and disruptive times.

Thank you to all our contributors, in this edition and over the past 20 years, and thank you, our readership, for your continued support!

Lance Levy, **Capco CEO**

COLLABORATING FOR THE GREATER GOOD: ENHANCING OPERATIONAL RESILIENCE WITHIN THE CANADIAN FINANCIAL SECTOR

FILIPE DINIS | Chief Operating Officer, Bank of Canada
Contributor: **INDERPAL BAL** | Special Assistant to the Chief Operating Officer, Bank of Canada

ABSTRACT

Parties in the Canadian financial sector share a high degree of interdependence and the threat landscape they face is ever changing. This means that an operational event, such as a cyber attack, affecting one institution can quickly spread to the wider sector. This article outlines some of the key elements of the Bank of Canada's role in promoting the operational resiliency of the financial system and the excellent collaboration taking place within the Canadian financial sector to enhance its collective resiliency posture. The Bank of Canada believes that the broad issues of resilience and vulnerabilities require a broad response, at the core of which is greater collaboration and information sharing. This has led the Bank to establish and lead the Canadian Financial Sector Resiliency Group (CFRG) and the Resilience of Wholesale Payments Systems (RWPS) initiative. Together, these efforts offer a forum for coordinating a national sectoral response to systemic operational incidents. They help the industry benchmark controls and processes, regularly test with crisis simulations, and enhance sector data resiliency to cyber attacks.

The CFRG and RWPS contributions attest to the sector's commitment to providing Canadians with a safer, more secure, and resilient financial system.

1. INTRODUCTION

If the pandemic has taught us anything, it is that extraordinary events do happen, and it is up to all of us to best prepare ourselves. In these unprecedented times, the old adage of "hope for the best, but plan for the worst" could not be more relevant.

Despite the impact of the pandemic on the global economy, we have witnessed many organizations demonstrate the kind of resilience we all ought to strive for. Be it transitioning to a remote workforce at the flip of a switch, swiftly enhancing measures to further bolster the health and safety of those performing critical on-site operations, or modifying existing processes to adapt to the new digital reality, we have seen how effective resiliency planning can pay dividends when the time comes.

Those organizations know all too well that being resilient does not just happen. It is the desired outcome of a series of specific and intentional efforts, investments, and collaboration that help ensure the best possible preparation for the unexpected. Being able to apply this lens beyond the walls of our respective organizations to benefit the greater collective can provide immense value to an industry, the participants within it, and those they serve.

The Bank of Canada plays a role in safeguarding the financial system against unforeseen events such as cyber attacks, and we take this role very seriously. To address the very real threats facing the financial sector, the Bank established and leads the Canadian Financial Sector Resiliency Group (CFRG) and the Resilience of Wholesale Payments Systems (RWPS) initiative. These efforts build invaluable partnerships for collaborating and breaking down barriers to information sharing. They represent an important step towards enhancing the sector's overall resilience. Of course, while we have made significant strides in working with both domestic and international partners more effectively and frequently, much work remains.

2. THE BANK OF CANADA'S ROLE AND RESILIENCY POSTURE

In its 86 years of existence, the Bank of Canada's core functions of monetary policy, currency, funds management, and the financial system have remained relatively constant. However, our exposure to risks, and the way in which we conduct our business, has evolved. For example, throughout most of the 20th century, central banks and individual institutions were more concerned with physical security and did not need to mitigate the cyber-related risks we face today [Dinis (2019)]. Indeed, at one point, the most prized possessions of a central bank were gold and currency; today it is data. What it takes to mitigate risks and be operationally resilient has evolved over the years. Many of the risks we face today are simply different or were nonexistent 30, 20, or even 10 years ago.

A central bank's resilience can have a direct impact on its ability to fulfill its mandates, and for this reason, the Bank of Canada has continued to make significant investments in this area. For example, our Business Recovery Enhancement program helps increase the resilience of our data centers, network and technology infrastructures, and business systems. This program helps the Bank remain resilient in the face of all types of operational events or shocks, ranging from weather-related to cyber incidents.

We have also invested in people, planning, infrastructure, and training to bring our new Calgary Operational Site online in 2019. Our Calgary staff are fully integrated with the banking and market operations team in Ottawa and can take over critical market functions at a moment's notice in the event of a major operational incident.

In addition, reflecting a best-practice governance model to align and coordinate cyber programs and activities, in 2018 we also introduced the position of the chief information security officer within the organization.

Given its dynamic nature, resiliency planning is a continuous process for the Bank, whereby we look for innovative ways to constantly enhance our posture. Our 2019-21 Cyber Security Strategy has been an important step in our cyber evolution [Bank of Canada (2019)]. It acknowledges that while much good work has been done, we have more to do to fulfill this mandate. This includes the continued enhancement of the security within our own operations, our ongoing collaboration with external partners to improve individual and collective resilience, and our leadership in promoting robust cybersecurity standards within the financial sector. Our next Cyber Security Strategy, which is currently under development, is expected to share many of these same objectives.

As the nation's central bank, whose mandate includes promoting the stability of the country's financial system, the Bank continues to prioritize operational resilience of the sector. In this context, our role is unique. We oversee critical financial systems, we play a key role in the operations and settlement of those systems, and we are also a participant within them. This being said, we recognize that the operational resilience of both the broader sector and the central bank is very much connected.

3. THE NEED FOR GREATER SECTORAL COLLABORATION

The broad vulnerabilities in the financial system today have the potential to exploit the high degree of interconnectedness of society, our economy, and our financial system. Consequently, we believe that these broad vulnerabilities require broad responses. When any organization thinks about its resiliency posture, such as its ability to recover from a cyber event, it is simpler to think of the implications within its four walls. It is relatively easy to quantify the risk, understand its impacts on operations, and then determine how much it should spend to mitigate that risk.

This analysis becomes much more complex when we expand it to include external stakeholders such as customers, vendors, and partners. However, this is also not broad enough since it does not take into account the systemic nature of the incident

[Dinis (2019)]. It does not consider that the incident could have severe implications for the wider sector, including financial institutions, networks, and even markets. The high level of interconnectedness of the financial system and its key players makes it difficult to quantify this risk. In efforts to mitigate such a risk, some players may be underinvesting as they are not considering its systemic nature, while others may be investing in the wrong areas. However, greatly enhancing the outcome for all, we believe the benefits from greater collaboration far exceed its costs.

When we look at the events to date relating to the global COVID-19 pandemic, it is easy to see just how far-reaching the implications of a breakdown in the resiliency of a single player within the financial system could be. For example, when the Bank of Canada began its intervention to support liquidity in key funding markets in March 2020 in response to the economic impacts of the pandemic, what came with it was a significant increase in the volume and value of transactions being carried out. The timely execution of these transactions was critical to support the economy. In fact, in just six months, the Bank of Canada's balance sheet increased from $120 billion on December 31, 2019 to $528 billion on June 30, 2020. Now, just imagine a hypothetical situation where there were vulnerabilities in the systems, networks, infrastructures, and key players involved. Vulnerabilities such as inadequate business continuity plans, the inability of existing systems and infrastructures to handle the sudden demands placed upon them, or worse yet, COVID-19 illness-related implications on staff. A situation where the increased volumes and values in transactions resulted in the inability of the central bank to provide timely, needed funding and liquidity to the markets. Such a situation could have had enormous impacts on not only the Canadian financial sector, but everyday Canadians as well.

This underscores the sentiments shared within the sector that maintaining the trust of Canadians is essential, as is having a well-protected financial system that can recover from an incident quickly with minimal damage. While controls and measures at individual institutions are an excellent line of defense, the complement of effective sector-wide actions are key to mitigating potential impacts to the broader system. These forces have been the driving purpose behind the creation and ongoing work of both the CFRG and RWPS initiative.

4. THE GREAT WORK OF THE CFRG AND RWPS

Launched in 2019, the CFRG is a public-private partnership. It brings together Canada's systemically important banks, financial market infrastructures, and the public sector, including the Department of Finance Canada, the Office of the Superintendent of Financial Institutions (OSFI), and the Canadian Centre for Cyber Security (CCCS). The mandate of the CFRG is to coordinate both resiliency initiatives and critical responses to systemic-level operational incidents within the financial sector.

The CFRG achieves its mandate in a few ways. First and foremost, it brings together key players in order to establish a playbook for coordinating a national, critical financial-sector response to systemic-level operational incidents. This includes a broad range of occurrences, from weather-related events to cyber incidents. With the ability to be activated on a moment's notice, this playbook serves as a mechanism for the broader sector to respond to an event in a coordinated, timely, yet effective manner, while minimizing its impact to stakeholders. Such an exercise informs decision-makers on the big picture to influence decisions that will benefit both the sector and Canadians. Second, the CFRG coordinates sector-wide resiliency initiatives such as benchmarking exercises and regular crisis simulations, the first of which was completed in March 2021. This recent crisis simulation included over 170 participants from member organizations and simulated the sector's coordinated response to a systemic operational incident. Such simulations provide the CFRG an opportunity to document and act upon key lessons learned and enhance its collective ability to respond to new and emerging threats. The CFRG's intent is not to direct or regulate how to make processes more resilient, but rather to bring both the private sector and government members together to share information and independently apply the lessons learned to their own internal processes. Lastly, the CFRG acts as a voice for the critical financial sector at related events and in other groups or committees, helping simplify the connections between government and the private sector.

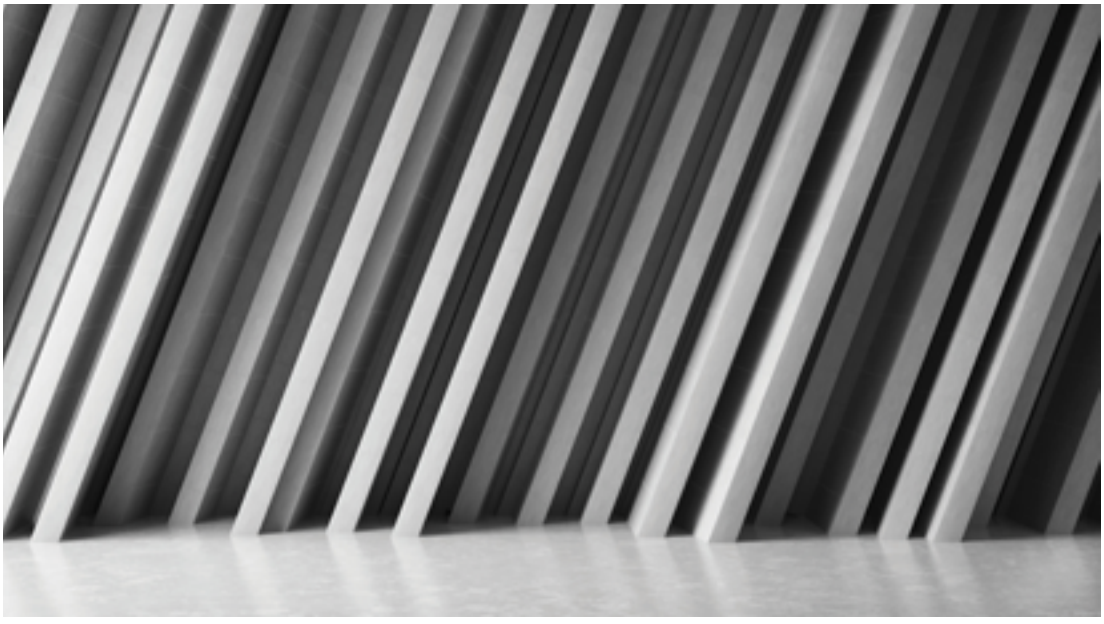
In fact, the CFRG has been heavily leaned on to steer the resiliency agenda throughout the COVID-19 pandemic. As the Canadian financial sector continues to navigate the impacts of the pandemic, the benefits of having a group such as the CFRG have become even more evident. The CFRG Steering

Committee has met on a regular basis to share status updates on COVID-19, emerging operational issues, and cyber threats [Bank of Canada (2020a)]. Committee members have shared information on business continuity plans and contributed to cross-government operational initiatives, such as the regular critical infrastructure discussions at the National Cross Sector Forum led by Public Safety Canada.

The RWPS initiative, also led by the Bank of Canada, is a public-private sector collaboration with Canada's largest banks as well as key providers of payment, clearing, and settlement systems. The objective of the RWPS is to enhance the wholesale payment sector's cyber resilience posture by: (i) improving controls across the sector that support payment data integrity; (ii) enhancing the maturity and effectiveness of cyber resiliency testing and the range of scenarios they cover; (iii) assessing and enhancing the capabilities to recover wholesale payment services in the case of a severe cyber event; and lastly, (iv) by maintaining a catalogue of cyber risk scenarios.

Cyber attacks are becoming more sophisticated and damaging, and harder to detect, than ever before. Not surprisingly, the Bank of Canada's most recent Financial System Survey [Bank of Canada (2020b)] highlighted the occurrence of a cyber incident as one of the top two risks to both individual firms and the Canadian financial system as a whole. Citing the increased reliance by firms on the new remote work environments, the survey also identified disruptions in information technology infrastructure as a significant risk. A cyber breach at one financial institution could spread and affect other institutions, networks, infrastructures, and markets, resulting in prolonged interruption and compromising data and, ultimately, consumer confidence. The industry recognizes that an effective sector-wide response must include greater sectoral collaboration and information sharing.

The collaboration taking place within the CFRG and RWPS initiatives enables the sector as a whole to more effectively and efficiently enhance its operational resiliency. As economists put it, by focusing on the collective good, the sector aims to avoid the "tragedy of the commons" [Dinis (2019)]. If individual organizations use shared, finite resources for their own needs first, then the common good suffers and everyone in the sector is worse off. Not only do these initiatives serve as a forum for information sharing, coordination, and allocation of workload, but they also enable the broader sector to benefit from the deep knowledge, expertise, and best practices shared by participant organizations. Furthermore, they build upon the strong relationships that participant organizations have with one another. These trusted relationships take time, energy, and resources to build, but we are confident that all will be better off as a result of the work taking place.



5. THE WAY FORWARD

So, what does the future look like for operational resilience in the context of the Canadian financial sector? First of all, the pandemic has put a spotlight on the need for the sector to continuously enhance its resiliency posture. The transition to remote work means that there is a much greater reliance placed on systems, infrastructures, and networks, and with this come additional risks. For example, firms rely more heavily on their staff to meet physical security safeguards at their home offices. Increasingly advanced and themed phishing attacks have targeted the remote workforce. Firms also have less control over ensuring that hardware and software remain up to date than if staff were on site.

We have seen the pandemic accelerate an already fast-moving train known as digitalization. Organizations have realized the potential of many emerging technologies and are more likely to default to a digital-first mindset now than ever before. This is particularly true in how technology and business procedures continue to evolve to support the remote work environment, rendering some existing assumptions not applicable in the future. This in turn may cause a need to revise existing plans. Consequently, the work of the CFRG and RWPS is far from done. Events and technologies are constantly evolving, and new emerging risks and opportunities need to be considered in both individual resilience planning and the context of the broader sectoral response.

Furthermore, new topics such as digital currency and blockchain continue to emerge. Central bank digital currency (CBDC) is on the radar of most central banks around the world. What new opportunities and risks could a CBDC bring to how we think about resiliency? What could it mean to be operationally resilient in the context of a financial system with a CBDC? These are just some of the questions that the broader sector may need to address.

Lastly, while we do think of the resiliency posture in the context of national borders, collaboration is also taking place at the international level. The Bank of Canada is an active member of numerous committees and organizations focused on aspects of global resilience and information sharing. The global community continues to increase the importance of operational resiliency and demonstrate the linkages to financial stability. As an example, the G7 continues work on cyber and operational resiliency as well as information sharing among member nations. This group recently published the "G7 fundamental elements of cyber exercise programmes" [HM Treasury (2020)].

6. CONCLUSION

The Bank of Canada's role in promoting the stability of the country's financial system continues to be a core function. The Bank has deep ties with the Canadian financial sector and a commitment to help it to be operationally resilient. The events pertaining to the COVID-19 pandemic have demonstrated that, for the ongoing recovery of the nation, a strong resiliency posture is critical for both the financial system as a whole and the participants within it.

The CFRG and RWPS support collaboration between public institutions – such as the Bank, OSFI, the Department of Finance, and CCCS – and the Canadian financial sector, including our financial market infrastructures. Participants are developing national critical financial sector responses to systemic-level operational incidents and simplifying the connections between government and the private sector. They coordinate crisis simulations, benchmarking exercises, and updates on operational issues. These initiatives are instrumental to a strong, resilient, and secure financial system able to withstand the impacts of operational events, including cyber attacks. While financial industry participants continue their work to build relationships and share information, we believe the sector is on the right path to advancing its shared agenda.

Maintaining the trust of Canadians is essential, and Canadian financial sector participants' commitment to these initiatives attests to that. Having a well-protected financial system that can recover from an incident quickly and with minimal damage is crucial. The Bank of Canada applauds the work and partnership of the sector and looks forward to continuing this engagement to promote the stability of the nation's financial system.

REFERENCES

Bank of Canada, 2019, "2019-2021 cyber security strategy: reducing risk promoting resilience," https://bit.ly/3t22T5E

Bank of Canada, 2020a, "Financial System Review – 2020: the impact of COVID 19 on the Canadian financial system," https://bit.ly/3mBxaGg

Bank of Canada, 2020b, "Financial System Survey highlights – November 2020," https://bit.ly/3s10wP8

Dinis, F., 2019, "Cyber security: breaking down barriers," remarks made to the Information Technology Association of Canada, Toronto, November 12, https://bit.ly/3wSvdtK

HM Treasury, 2020, "G-7 fundamental elements of cyber exercise programmes," policy paper, December 28, https://bit.ly/3wwEcRb

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO