THE CAPCO INSTITUTE
JOURNAL
OF FINANCIAL TRANSFORMATION

TECHNOLOGY

Why cyber resilience must be a top-level leadership strategy

STEVE HILL | SADIE CREESE

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

08 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

14 Preparing for critical disruption: A perspective on operational resilience
Sanjiv Talwar, Assistant Superintendent, Risk Support Sector, Office of the Superintendent of Financial Institutions (OSFI)

18 Operational resilience: Industry benchmarking
Matt Paisley, Principal Consultant, Capco
Will Packard, Managing Principal, Capco
Samer Baghdadi, Principal Consultant, Capco
Chris Rhodes, Consultant, Capco

24 Decision-making under pressure (a behavioral science perspective)
Florian Klapproth, Professorship of Educational Psychology, Medical School Berlin

32 Operational resilience and stress testing: Hit or myth?
Gianluca Pescaroli, Lecturer in Business Continuity and Organisational Resilience, and Director of the MSc in Risk, Disaster and Resilience, University College London
Chris Needham-Bennett, Managing Director, Needhams 1834 Ltd.

44 Operational resilience approach
Michelle Leon, Managing Principal, Capco
Carl Repoli, Managing Principal, Capco

54 Resilient decision-making
Mark Schofield, Founder and Managing Director, MindAlpha

64 Sailing on a sea of uncertainty: Reflections on operational resilience in the 21st century
Simon Ashby, Professor of Financial Services, Vlerick Business School

70 Operational resilience
Hannah McAslan, Senior Associate, Norton Rose Fulbright LLP
Alice Routh, Associate, Norton Rose Fulbright LLP
Hannah Meakin, Partner, Norton Rose Fulbright LLP
James Russell, Partner, Norton Rose Fulbright LLP

TECHNOLOGY

80 Why cyber resilience must be a top-level leadership strategy
Steve Hill, Managing Director, Global Head of Operational Resilience, Credit Suisse, and Visiting Senior Research Fellow, King's College, London
Sadie Creese, Professor of Cybersecurity, Department of Computer Science, University of Oxford

84 Data-driven operational resilience
Thadi Murali, Managing Principal, Capco
Rebecca Smith, Principal Consultant, Capco
Sandeep Vishnu, Partner, Capco

94 The ties that bind: A framework for assessing the linkage between cyber risks and financial stability
Jason Healey, Senior Research Scholar, School of International and Public Affairs, Columbia University, and Non-Resident Senior Fellow, Cyber Statecraft Initiative, Atlantic Council
Patricia Mosser, Senior Research Scholar and Director of the MPA in Economic Policy Management, School of International and Public Affairs, Columbia University
Katheryn Rosen, Global Head, Technology and Cybersecurity Supervision, Policy and Partnerships, JPMorgan Chase
Alexander Wortman, Senior Consultant, Cyber Security Services Practice, KPMG

108 Operational resilience in the financial sector: Evolution and opportunity
Aengus Hallinan, Chief Technology Risk Officer, BNY Mellon

116 COVID-19 shines a spotlight on the reliability of the financial market plumbing
Umar Faruqui, Member of Secretariat, Committee on Payments and Market Infrastructures, Bank for International Settlements (BIS)
Jenny Hancock, Member of Secretariat, Committee on Payments and Market Infrastructures, Bank for International Settlements (BIS)

124 Robotic process automation: A digital element of operational resilience
Yan Gindin, Principal Consultant, Capco
Michael Martinen, Managing Principal, Capco

MILITARY

134 Operational resilience: Applying the lessons of war
Gerhard Wheeler, Head of Reserves, Universal Defence and Security Solutions

140 Operational resilience: Lessons learned from military history
Eduardo Jany, Colonel (Ret.), United States Marine Corps

146 Operational resilience in the business-battle space
Ron Matthews, Professor of Defense Economics, Cranfield University at the UK Defence Academy
Irfan Ansari, Lecturer of Defence Finance, Cranfield University at the UK Defence Academy
Bryan Watters, Associate Professor of Defense Leadership and Management, Cranfield University at the UK Defence Academy

158 Getting the mix right: A look at the issues around outsourcing and operational resilience
Will Packard, Managing Principal, and Head of Operational Resilience, Capco

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**

WHY CYBER RESILIENCE MUST BE A TOP-LEVEL LEADERSHIP STRATEGY

STEVE HILL | Managing Director, Global Head of Operational Resilience, Credit Suisse, and Visiting Senior Research Fellow, King's College, London

SADIE CREESE | Professor of Cybersecurity, Department of Computer Science, University of Oxford

ABSTRACT

Cyber resilience is a critical and hard to achieve facet of operational resilience. Trends in digital technology use and evolution of the threat ecosystem are amongst the drivers likely to make it increasingly more urgent, and difficult, to deliver. This article reflects on our current vulnerability, how global politics interplays with organizational risks, and the systemic issues we face. It argues that a renewed effort to enhance cyber resilience, as distinct from increasing data protection, is needed at both governmental and enterprise leadership levels.

1. INTRODUCTION

Over the last decade, the media cyber drumbeat has become familiar: U.S. and Israel disruption of the Iranian nuclear program (2010); Iranian attacks on Saudi Aramco production – constituting 10 percent of global oil supply (2012; 2017); Russian cyber attacks on the power grid in parts of Western Ukraine, leaving almost a quarter of a million Ukrainians without power for several hours (2015; 2016); the failure of major U.S. internet platforms and services after the domain name system (DNS) provider, Dyn, was victim of a series of distributed denial of service attacks carried out by a group of juvenile hackers (2017); the disruption of tens of thousands of travel plans when a BA data center stopped working (2017); almost 1.9 million TSB bank customers in the U.K. being locked out of their accounts and unable to bank online following a botched migration to a new IT platform (2018); the SolarWinds attack (2020), and, most recently, the attacks on Microsoft Exchange servers (2021), creating backdoors into the networks of numerous businesses and governments. The latter demonstrated the degree to which a malign network presence can endure undetected. A 2017 Freedom of Information request sent to U.K. Critical National Infrastructure firms found that over a third of their IT outages were caused by cyber attacks,[1] a statistic that is borne out by the increasing volume of incidents reported worldwide, the impact of which are yet to be fully understood.

Operational resilience has become a major policy and business focus, and in our increasingly digitized world, cyber resilience is the most critical facet of this. Yet, the preoccupation with ever-larger personal data breaches has overshadowed what may ultimately be a more existential threat to our societies and citizens: system loss rather than data loss. This paper demonstrates our current vulnerability and argues that a renewed effort to enhance cyber resilience, as distinct from increasing data protection, is needed at both governmental and enterprise levels. Leaders need to strengthen our ability to withstand cyber and technology shocks across the wider Critical National Infrastructure.

2. KEY DRIVERS

We know that there is no possibility of guaranteed security. The practice of cybersecurity is inherently about managing cyber risk so that the exposures are acceptable and our organizations can survive incidents, i.e., to deliver resilience. The need to revisit how we achieve such resilience is driven

[1] Nominet Cyber Security, 2017, "Why critical national infrastructure (CNI) providers need CNI-ready DNS security," https://bit.ly/3tdCa5M

by changes in our business operations, our need to adopt new technology and embrace the opportunities they bring, and by the continued investment in attack capability by the threat ecosystem:

1. Digitization continues to accelerate, given yet another adrenaline boost by the 2020 COVID-19 pandemic. Reliance on a small number of internet service and cloud providers is growing exponentially. The shift online will only continue, fueled by the arrival of 5G and the development of the "internet of things". As big iron and big data elide, the distinctions between the physical and virtual worlds in the fourth industrial age will continue to dissipate, further challenging our ability to define boundaries and protect perimeters.

2. As this shift occurs, attack surfaces will continue to expand across our digital and business systems. We must change the paradigm to ensure security is no longer traded off for efficiency and speed. Complexity and external dependencies, many of them unsuspected or hidden, will grow. We will continue to discover new dependencies and vulnerabilities within our ecosystems, and consequentially risk will aggregate.

3. Our compliance regimes will try to reduce vulnerability and exposure to losses but may not shift sufficiently towards a risk-based approach, thus making it increasingly difficult to scale up and meet the challenge. Business leadership will seek to demonstrate a principled approach, not least to maintain defensible positions in the face of costly incidents.

4. Meanwhile, we will be faced by the continued industrialization of cybercrime. Cyber weaponry will continue to proliferate globally and will be largely undeterred with organized criminal groups, often operating from safe havens beyond the reach of law enforcement, demonstrating enviable innovation and agility.

5. Increasing numbers of governments, looking at the success of Russia, China, Iran, and the DPRK, will take advantage of the low threshold for offensive cyber capabilities and take advantage of the grey space that hybrid warfare offers.

6. Even without malign actors, secure change management in a world of increasing complexity will continue to prove all but impossible. We will be forced to evolve but things will go wrong.

3. SYSTEMIC IMPORTANCE

At a state level, Russia has led the way in demonstrating the potential of leveraging deniable cyber capabilities to achieve real world impact (Estonia, Georgia, and Ukraine). SolarWinds has been yet another reminder of the degree to which Russian capability and willingness to use it should not be underestimated. Russia may have been taken aback by the scale of the NSA operations that Edward Snowden betrayed, but the next shock looks more likely to be in the opposite direction. The U.S. may, as President Obama boasted, have had "more capacity than anybody both offensively and defensively," but Russia appears to have the determination to operationalize their capabilities. Even worse, the U.S. persists in prioritizing offence over defense. Some U.S. officials still argue for back doors to be built into end-to-end encryption. The U.S. government has openly acknowledged that Russia has established footholds in their power infrastructures and, in a version of the nuclear mutually assured destruction (MAD) doctrine, have all but admitted that they have the capability to penetrate those of others. The contamination of the water supply of a small Florida city by a hacker, who broke into the software controls earlier this year to increase the levels of sodium hydroxide to more than a hundred times the safe limit, was yet another reminder of the potential threat.

The global political environment has always mattered to business, since international relations determine, in part, trade environments and regulatory regimes. However, cyber adds a new dimension as the capability developments made by governments eventually filter out into the wider threat actor ecosystem. This will include the development of intelligence on targets, supplies of software tools and knowledge used to conduct attacks, human manpower capacity to conduct campaigns that require persistence and remote control, and maintenance of teams and facilities with the ability to swiftly action requests. In other instances, these same capabilities indirectly make their way into the wider ecosystem. Regardless of the process of knowledge and tools transfer, the effect is the same – a tangible and continued evolution of cyber-attacker capabilities that will be used against commercial businesses and national critical infrastructures.

Global politics is not, however, the only systemic issue we face. Our societies rest upon a digital foundation every bit as critical as our transportation, health, electricity, water, and sewage systems. The constant evolution of our organizations towards becoming digitized is making the digital services layer a part of critical infrastructures, as are the devices that we increasingly use in instrumenting our control systems and global supply chains. Yet, government oversight is sparse. Cloud providers, partly because they have not suffered the same outages as the financial services sector, have been largely immune from governmental regulations. Commercial drivers – and an aspiration to 'five nines' (99.999 percent) reliability – is seen as a sufficient driver to resilience.

History has shown us that commercial drivers alone will not deliver a digital infrastructure free from attack surface, which means that it will be for the users of that digital infrastructure to deliver resilience knowing that they are exposed to risks because there is always a way for attackers to successfully penetrate our systems.

4. ENTERPRISE LEVEL

National infrastructure largely comprises of private enterprises, seeking to increase shareholder value and – very often – increase efficiencies by reducing costs. Their IT infrastructures are typically a Kluge of legacy systems and external third party dependencies organically grown through acquisition and evolution. In challenging economic times, investing against possible, but unlikely, risk events has not been a priority. This has become apparent when such events, whether malicious ransomware attacks or botched IT transitions, have occurred. Customers have often been the ones to suffer the consequences. It is conceivable that such risk events will be considered ever more likely in the future, making the choice not one of whether to invest, but rather how much to invest and which capability will produce the best security returns.

Regulators, especially in the financial services industry, have sought to redress the balance. As banks have shifted from bricks and mortar to online digital services, regulations are imposing responsibilities on banks to ensure that critical business services will be resilient even when faced with severe, but plausible, stress scenarios. The European Union's Digital Operational Resilience (DORA)[2] draft legislation extends this wider, and the E.U.'s Cybersecurity Strategy for the Digital Decade (December 2020)[3] points to a significant investment in cybersecurity operations capability. However, implementation will inevitably be patchy and offer limited protection across supply chains. Hence, whilst business can expect an eventual enhancement in capacity, through new risk controls supported by regulatory and principled guidance, these initiatives cannot be a panacea for delivering cyber resilience.

5. CURRENT RESPONSE

Corporate boards, supported by increasingly experienced chief information security officers (CISOs) and chief information officers (CIOs), understand the challenge. Cyber is rarely outside the top five of any enterprise risk register. In most multinationals, technology risk is regularly discussed and is no longer delegated to the IT team; business continuity cyber scenarios are regularly practiced, with general counsel, regulatory affairs, insurance managers, and corporate communications experts all fully engaged.

Boards recognize that perimeter security no longer suffices, and that walls can easily become eggshells. Cyber incidents should be assumed, and insider threats anticipated and monitored for. There has been a paradigm shift away from traditional non-financial risk management and business continuity planning that focused on lagging incident metrics, which could give an unduly reassuring picture based on measuring levels of activity rather than actual improvements in security posture, towards more of a proactive focus on creative scenarios that can anticipate new threats. In his recent book, "The fifth risk", Michael Lewis[4] describes the challenges of those predicting tornadoes in the U.S. Midwest, where the data science has improved significantly but populations remain strangely resistant to responding to their warnings. By the same token, could it be that cybergeddon will occur before resilience is afforded the status it deserves?

COVID-19 highlighted the degree to which risk experts underestimate extreme tail-end risks; or at least how little they are able to influence policy-makers to act on these. For the most part, as the former Speaker of the Texas House said in the aftermath of the February 2021 weather-caused power outages, "we knew what to do; we just didn't do it."[5] The impressively agile private sector response, enabling a rapid

[2] https://bit.ly/3t2gWI1
[3] https://bit.ly/3bBqSCv
[4] Lewis., M, 2018, The fifth risk, W. W. Norton & Company
[5] https://econ.st/3qDShIn

shift to working from home, should not disguise the failure to prepare for a global threat of this magnitude. It was no black swan – it was rather a black elephant (in the room) that had been willfully ignored by boards, governments, and think tanks overwhelmed by more recent and familiar challenges, or by those risks determined to be more likely, where the return on mitigation investment will be easier to evidence.

Global financial regulators, led by the Bank of England, have sought to redress this underestimation by signaling that they will, from 2022, impose an expectation of operational resilience for the important business services provided by the financial services sector on which citizens increasingly depend. Financial institutions are identifying which of their business services are critical to their clients or to the wider financial system. They are embarking on extensive exercises to map the business processes and dependencies that underpin each of these services and putting stress testing programs into place to assess whether, faced with severe but plausible scenarios, the services can be recovered within an 'impact tolerance' that the bank judges to be reasonable. These new programs are major new undertakings, building on the lessons learnt during the 2020 response to the global COVID-19 pandemic.

6. RESILIENT BY DESIGN

Looking forward, there are signs of a greater awareness of these systemic threats and the need to build long-term cyber resilience. The current response is necessary, but not necessarily sufficient. One size will no longer fit all: the best response to a loss of physical premises (a hot-hot production/ disaster recovery set-up) might very well be exactly the wrong response to a sustained malware attack. When faced with cyber attacks we cannot assume standard failure rates of a benign environment, instead we are faced with the creativity of threat actors who are motivated and will innovate to succeed. It is extremely difficult to stress-test for all possible futures that might bring, especially given the inextricable links to global politics and economic outcomes.

The robust response from the Trump Administration to the potential threats posed by embedding Huawei technology into 5G networks may signal a change of priority. Convenience and cost do not always have to prevail. Just as CISOs talk of new systems needing to be "secure by design", there is also a recognition that future systems and processes, both at enterprise and Critical National Infrastructure level, will need to be "resilient by design". Emerging technologies, such as distributed ledger technology, cloud-based data vaulting, or digital twinning capabilities may provide responses by which we might bolster our resilience,[6] but they may also prove to be new sources of vulnerability and hidden aggregation of risk.

Some of the response can only be delivered at governmental level. The new Biden Administration may be more minded to create more of an environment to develop international cybersecurity norms, even if this can only be done in certain like-minded jurisdictions initially. A greater focus on attribution and retribution for state cyber attacks might erode the sense of impunity and empowerment of those government agencies or organized criminal gangs operating from hostile jurisdictions. Intelligence agencies may need to reprioritize their defensive over their offensive capabilities. The Biden Administration may also help reverse the retreat from globalization, and the mutual economic entanglements that encourage greater global resilience. No major state actor has an incentive to attack infrastructure that serves itself as well as the rest of the world: entanglement by design may represent a significant insurance policy. However, hidden systemic cyber risks will continue to offer the potential for significant harm.

7. CONCLUSION

Achieving cyber resilience will necessitate a holistic approach across government and the private sector, driven by cybersecurity and intelligence experts. Only top leadership, in Cabinet and on boards, will be able to drive the recognition of the degree to which digital is central to 21st century life and pull together the strands needed to significantly enhance our resilience. Greater sharing of lessons and experiences both between enterprises and between governments, notwithstanding potential reputational consequences, will be critical to collective progress. Our leadership will need to become adept at adapting to new risks, pioneering new controls, investing in the capacity to change, and innovate in cybersecurity practice simply to maintain resilience. Without a strong leadership this level of dynamism will be impossible to achieve.

[6] The U.S. Safe Harbor program demonstrates how innovative new thinking, as well as new technology, can support this initiative.

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