Technology Risk and Regulatory Compliance

Impact During COVID-19

August 2021

By Pauline Wray, Alain Schneuwly, Sugar Chan, Maneet Ahuja, and Donovan Choy

BCG

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

Expand was founded in 2001 and is a fully-owned subsidiary of the Boston Consulting Group with headquarters in London and regional offices in New York and Singapore.

Expand has established its credibility as a trusted adviser to executive teams of financial institutions, offering research and syndicated benchmarking for the world's leading firms. Through its unique decision support and research services, Expand enables the development, validation and execution of better strategies across business lines and functions, helping organisations grow, compete and operate more effectively. Our delivery teams provide unrivalled levels of industry experience in financial markets and a unique perspective on solving problems associated with researching, sourcing and implementing new and innovative solutions.

Technology Risk and Regulatory Compliance

Impact During COVID-19

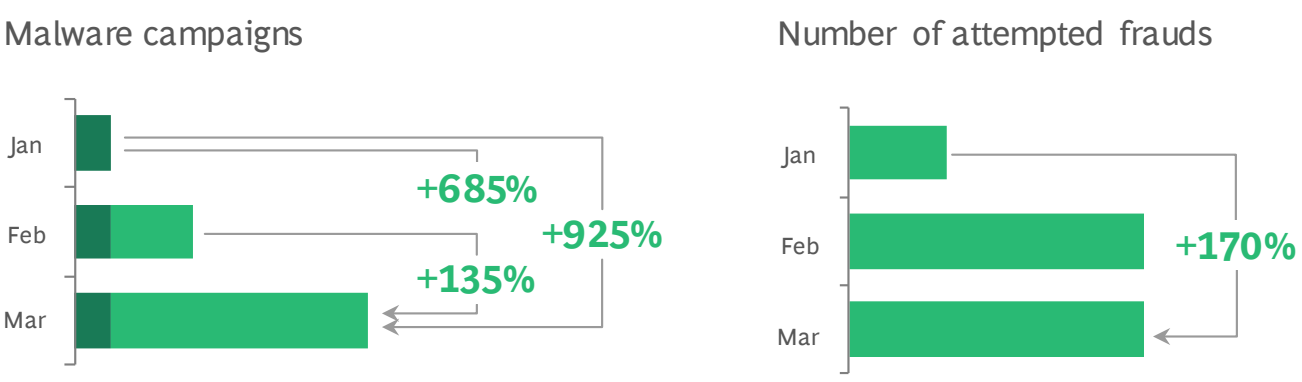
As the COVID-19 virus swept across the world early 2020, the global workforce went into lockdown. Financial Institutions were required to activate their business continuity plans. Employees were thrusted into a work-from-home environment and organizations had to ensure that proper controls and processes were in place, and in line with security and compliance requirements. The resilience of Technology Risk and Information Security functions of Financial Institutions were put to the test. As virtual workloads increased, banks faced the challenge of sustaining a high volume of users in a remote working arrangement. Regulatory scrutiny of banks' risk management frameworks was increased.

This white paper by BCG's subsidiary Expand Research is a summary of the impact of COVID-19 on the Technology Risk and Information Security functions of Banking in APAC. The first section details the impact on different areas of technology risk, from remote access and voice recording compliance, insider threats and more. The second section provides an overview of the regulators' response. The final section concludes with implications for Financial Institutions moving forward.

01 COVID-19 impact on cybersecurity and technology risk

In the immediate wake of COVID-19, cybersecurity arose as one of top five enterprise risks for C-suite management and board members. On a list of "clear and present dangers", the 2021 World Economic Forum report found cybersecurity failure to be the 4th highest after infectious diseases, livelihood crises and extreme weather events.[1] This is no surprise. Cybersecurity threats are not new and are only now exacerbated by work-from-home arrangements. One global bank reported between January and April of 2020 a historically unprecedented record of cyber-attack attempts; there was a 925% increase of malware campaigns and 170% attempted fraud scams. The number of malicious websites blocked daily also jumped from five to 12 - a 140% increase.[2]

Exhibit 1 - Large European bank faced increased cyber-attack attempts

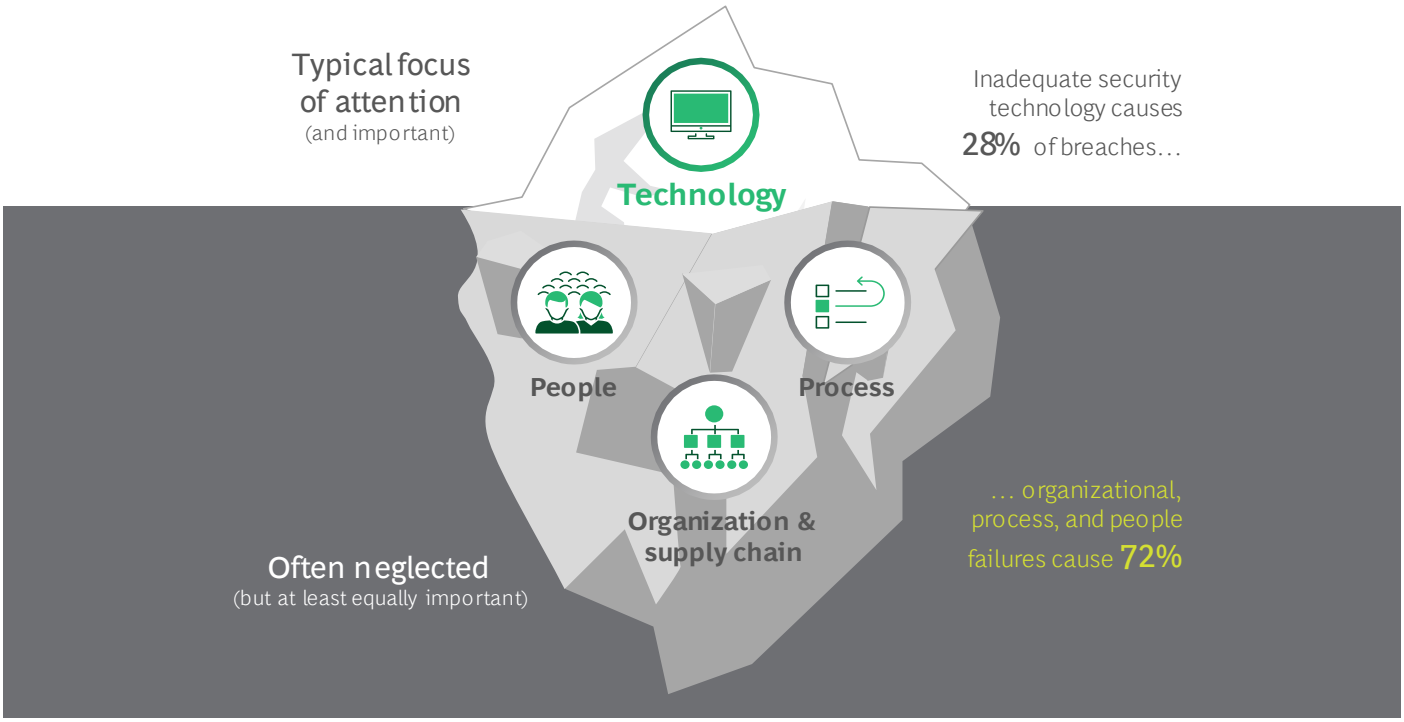


Source: Boston Consulting Group

1. https://www.weforum.org/reports/the-global-risks-report-2021
2. Boston Consulting Group

The type and magnitude of cyber threats largely depend on a robust cyber governance operating model in addition to the set of technological tools that financial institutions use. As illustrated in exhibit two, BCG found that 72% of security breaches stemmed from non-technology issues such as people, organization and processes, contrary to popular opinion that the problem is predominantly one in technology. As such, adapting to this new normal has no one-size-fits-all template, and would vary depending on existing setups.

Exhibit 2 - Security breach is an organizational challenge, not just technology



Source: Boston Consulting Group

This section of the white paper looks at the various technology risks that our surveyed banks faced last year.

Business Continuity Planning

> "Due to our large and complex organization, an extensive exercise was initiated to better understand each jurisdiction's capabilities. This enabled us to drive operational efficiencies as our working model shifted due to COVID-19. – Regional Head of Cybersecurity

As governments across Asia-Pacific began issuing work-from-home mandates, employees started relocating to home environments, while some banks in Hong Kong, Japan and Singapore continued to have exceptions for roles that required the use of onsite physical terminals, such as traders, or the use of a secure network for regulatory submissions.

The most immediate challenge for banks to move to a work-from-home mode was to cope with the inadequacy of existing cyber crisis management plans, which lacked scenario plans on the scale of a pandemic. Work-from-home measures were adopted in all countries where banks had their operations. As such, the organizational strategy of shifting work to offshore locations was rendered irrelevant.

Remote access

As remote working became the norm, remote access measures were revisited to reduce data leakage risks. From the banks that Expand interviewed, the common, bare minimum security controls were already in place, such as privileged identity and access management, mobile device management, disabling of USB ports and prior approval processes. On top of that, financial institutions also implemented advanced controls to ensure security over remote access. Examples of these measures include establishing new protocols for remote working behavior, providing tailored security for higher risk organizational roles, and updating cybersecurity detection for remote work patterns.

A larger concern emerged around remote information access by third-party vendors such as external consultants and contractors due to the way they might be accessing critical information through unsecure networks or devices.

Exhibit 3 - MAS Technology Risk Management Guidelines timeline

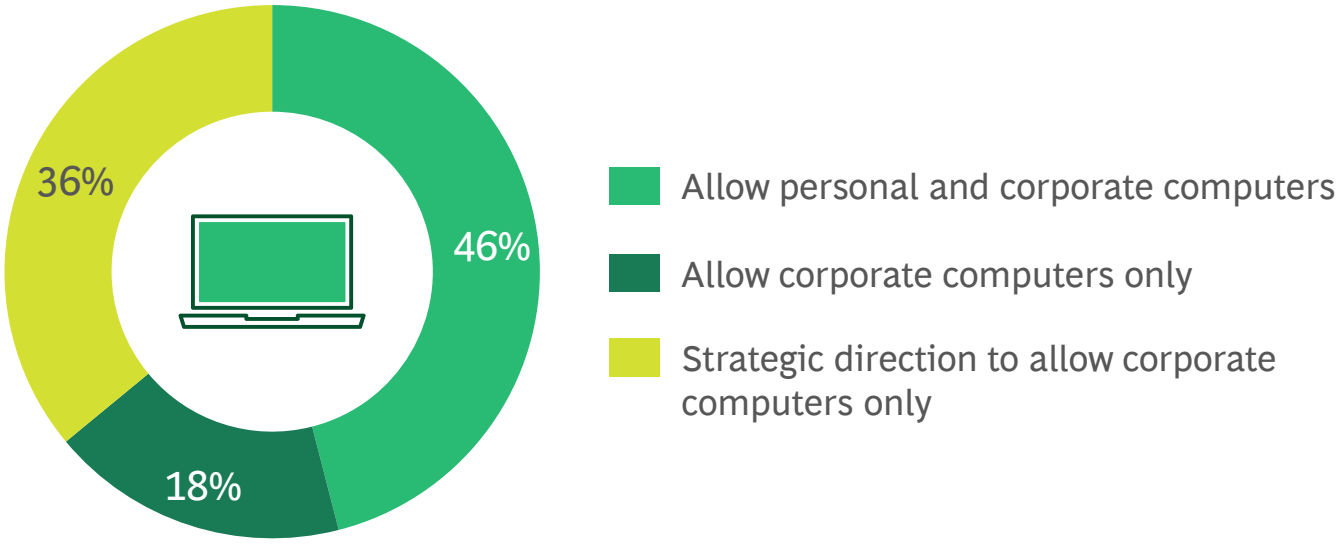
Source: Expand Research

This is consistent with the requirements in the Monetary Authority of Singapore's (MAS) updated Technology Risk Management Guidelines (TRMG) around third-party vendor governance, which emphasizes financial institution's employ stronger oversight and a "high standard of care and diligence" to protect against potential systemic and data risks.[3] In November 2020, the MAS has also urged banks to maintain oversight of all external third-party vendors that would require access to the banks' IT systems or data within its network.[4]

Moving into the new normal, regulators continued to enforce security controls for remote access to company networks, as seen in an advisory standard on remote working security that was issued by India's regulators.[5] Expand surveyed Regional Technology Risk Heads of 14 banks and found that while most continued to allow both corporate and personal devices, 36% are looking to transition to only allow access through corporate devices, in order to curb security and data leakage risks of working on personal devices.

3. https://www.mas.gov.sg/news/media-releases/2021/mas-enhances-guidelines-to-combat-heightened-cyber-risks
4. https://www.mas.gov.sg/news/media-releases/2020/financial-institutions-need-to-review-security-controls-amidst-covid19
5. https://www.bseindia.com/markets/MarketInfo/DispNoticesNCirculars.aspx?Noticeid={82D062CB-B1EB-49C9-ABC1-E5528302BCC4}&noticeno=20201030-16&dt=10/30/2020&icount=16&totcount=16&flag=0

Exhibit 4 - Bank's policy on the use of personal computers



Source: Expand Research

Voice recording compliance

Voice recording also posed compliance complications. Remote working meant that conversations that required recording for compliance purposes via trading turrets or dealer boards, could not be done or were conducted in an uncontrolled home environment. To some extent, this was mitigated for traders using Bloomberg terminals which recorded and stored trader conversations. Alternatively, banks with corporate-issued phones leveraged solutions such as VoxSmart to comply with mobile voice recording regulatory requirements.

VPN connectivity and latency

Latency and performance issues surfaced. VPN capacity was overloaded from a spike in remote usage, rendering inconsistent network performance. All banks reported an overall volume increase for IT support, with one Bank experiencing increase in online tickets and live chat support requests by 500%. The implications for time-sensitive trading functions such as cash FX trades, where a mere matter of seconds might make or break a deal, necessitated that traders continued working from the office until VPN issues were stabilized.

Remote working solutions

> **Many digitization projects were already in the pipeline, but COVID-19 helped to overcome organizational inertia and accelerated many of them.**
> **– Regional Head of Technology Risk**

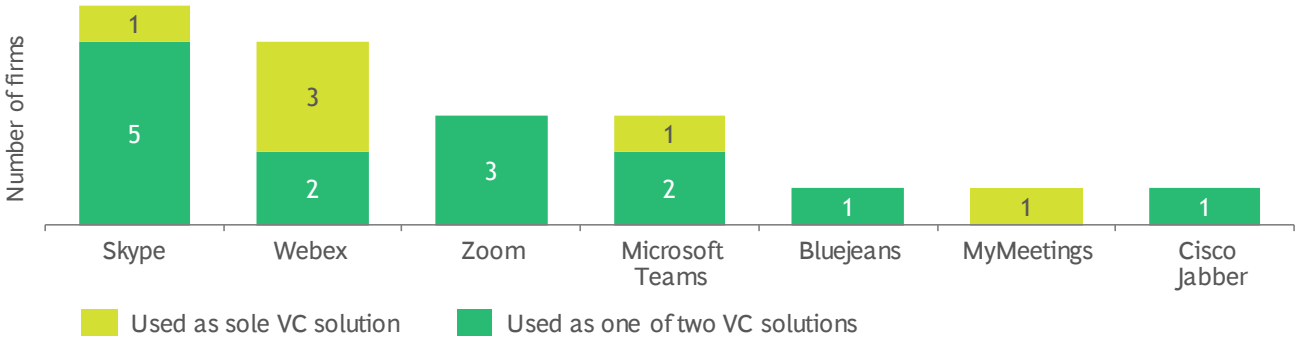
Remote work tools were widely onboarded in banks, and technological offerings were expanded to enable the continuous servicing of customers and clients. According to the HR Reporter, spending during COVID-19 hit a record US$15 billion extra per week on technology to enable safe and secure home working during COVID-19.[6] For instance, the inability to collect wet signatures while working from home led to the rolling out and expanding of e-signature and document management solutions. DocuSign, whose valuation soared in 2020, was the most commonly cited e-signature solution by the surveyed banks along with E-sign, OneSpan and Adobe Sign.

Printing from home was subject to a strict case-by-case approval and exceptions process to reduce information security risks. As a result, the need to print was predominantly carried out by onsite staff.

The use of web conferencing tools was also expanded. Although Zoom continues to be the most cited videoconferencing platform in the media, the survey found that 30% of banks had restricted the use of Zoom citing security concerns, opting in favor of solutions such as Microsoft Skype, Cisco Webex, Microsoft Teams, and to a smaller extent Verizon's Bluejeans, MyMeetings and Cisco Jabber.

6. https://www.hrreporter.com/focus-areas/hr-technology/cybersecurity-professionals-in-high-demand-as-attacks-surge-report/333565

Exhibit 5 - Video conference solutions used



Source: Expand Research

Insider threats

Finally, a spike in phishing attacks and insider threats have driven banks to reevaluate their existing insider threat and information security controls. Insider threats are not to be underestimated. According to the IBM Security's 2020 Cost of Insider Threats Global Report, there was a recorded 4,716 insider threat incidents across thirteen verticals.[7] This represents a half-fold increment (47%) from the baseline of 3,200 incidents in 2018. The overall costs of insider threats saw a significant 31% increase from $8.76 million to $11.45 million in the same period.

Our surveyed banks conducted reviews of existing legacy preventative controls such as network monitoring and activity review at the application level, and rules-based monitoring of email traffic to understand data loss prevention (DLP) behavior. Existing privileged ID management controls were reassessed to ensure robust authentication measures and access logging for appropriate employees and systems containing critical data; the most mentioned solutions include HiPAM and CyberArk.

WHO LED YOUR DIGITAL TRANSFORMATION?

1. CEO
2. CIO
3. COVID-19

There was a clear investment push in analytics-based tools such as Splunk and Behavox to better combat insider threats. Banks mentioned the use of robotic process automation (RPA) solutions to reduce human error involved in email attachments, while machine learning technologies helped to understand unusual remote working user behavior. At least half the banks Expand spoke with acknowledged that COVID-19 did not necessarily lead to the start of new projects, but instead accelerated or reopened digitization projects that were in the pipeline. Commonly mentioned projects included Microsoft Office 365, VPN gateway upliftment and tightening of cyber and security controls. As the joke goes, the digitization journey in 2020 is primarily driven not by CEOs or CTOs, but by COVID-19.

02 REGULATORY ACTIVITY

What actions did regulators take?

APAC regulators encouraged banks to quickly transit into remote working arrangements. As banks rushed to ensure that requisite controls were in place during work from home, extensions to deadlines of some major regulatory notices were observed while on-site inspections were postponed and placed on hold.

7. https://www.ibm.com/security/digital-assets/services/cost-of-insider-threats/#/

Exhibit 6 - Major regulatory extensions in 2020

Country	Regulatory Authority	Extensions
Australia	APRA (Australian Prudential Regulation Authority)	CPS234 third-party information security requirements[8]
Hong Kong	HKMA (Hong Kong Monetary Authority)	Submission for Consultation paper for HKMA CFI 2.0[9]
Hong Kong	SFC (Securities and Futures Commission)	Enforcement date for SFC EDSP requirements[10]
Singapore	MAS (Monetary Authority of Singapore)	Various deadlines pushed back[11]

Based on Expand's data, the average monthly onsite inspections across APAC region during the peak COVID-19 months declined. Inspections from regulators only resumed gradually from June.

> **During the period March to September 2020, inspections were 29% lower when compared to the same period in 2019.**

However, a spike in ad-hoc regulatory activity was also observed over the same time-period. Regulators such as MAS, HKMA and APRA were actively engaging technology risk personnel for weekly touchpoints. Advisories and surveys (see figure one) were issued, predominantly targeted at the types of cybersecurity controls that banks deploy in a remote working environment. Regulators sought to ensure that cyber risks were well managed, and guidelines were issued on best practices related to remote work.

8. https://www.apra.gov.au/news-and-publications/apra-announces-new-commencement-dates-for-prudential-and-reporting-standards
9. https://www.hkma.gov.hk/eng/regulatory-resources/regulatory-guides/circulars/?t=1607485531311
10. https://apps.sfc.hk/edistributionWeb/api/circular/openFile?lang=EN&refNo=20EC26
11. https://www.bovill.com/covid-19-mas-pushes-back-deadlines/

Exhibit 7 - Advisories and surveys issued during lockdowns

Regulator	Description
APRA (Australian Prudential Regulatory Authority)	• Request for information on pandemic stress scenarios
PBOC (The People's Bank of China)	• ASIFMA coordinated an information request from PBOC on industry actions in light of COVID-19 and also impact on business • PBOC requested a bi-weekly report on financial support to the individual and company clients impacted by COVID-19
CBIRC (China Banking and Insurance Regulatory Commission)	• CBIRC requested banks to provide update on adjustment of business development plans and management strategies for 2020
RBI (Reserve Bank of India)	• RBI issued alert to reiterate measures to be taken to counter threats from certain nation state actors regarding information sharing to detect and defend against cyber threats, and implementing best cybersecurity practices
BSP (Bangko Sentral Ng Pilipinas)	• Memo from BSP regarding surveillance measures/actions put in place by bank to manage growing cyber-criminal activities due to COVID-19
MAS (Monetary Authority of Singapore)	• MAS requested an ad-hoc call with Country Executive and Compliance to discuss the minimum on-site staffing requirements for critical functions • MAS Survey on Enhanced BCP Measures in response to the 2019 Novel Coronavirus • MAS Advisory on Technology Risk Management During COVID-19 Situation - 3 sections – Split Operations and Telecommuting; Staff Security Awareness; Customer Awareness
BOT (Bank of Thailand)	• BoT issued insights on best practices for IT preparations during the outbreak of COVID-19 • BoT expressed concerns via email on cyber security risk exposed to the banks systems; In addition, BOT also attached "Remote access Tips & Tricks" from several experts and supervisors for reference in maintaining IT security of the bank

Note: Non-exhaustive

Regulator's requests for information spanned across a wide variety of technology risk topics and changed as the situation with COVID-19 evolved. Initial enquiries ranged from controls around remote access to business continuity management measures in the event of further lockdowns. Throughout the year, APAC regulators placed a strong focus on cybersecurity measures with rising phishing and impersonation attacks.[12]

Expand found that one-fourth of all banks' regulatory interactions in 2020 comprised of activities related to COVID-19. The questionnaires, surveys and enquiries were mainly in the areas of cybersecurity, technology risk management and business continuity management.

Exhibit 8 - Supervisory activity experience by banks in APAC

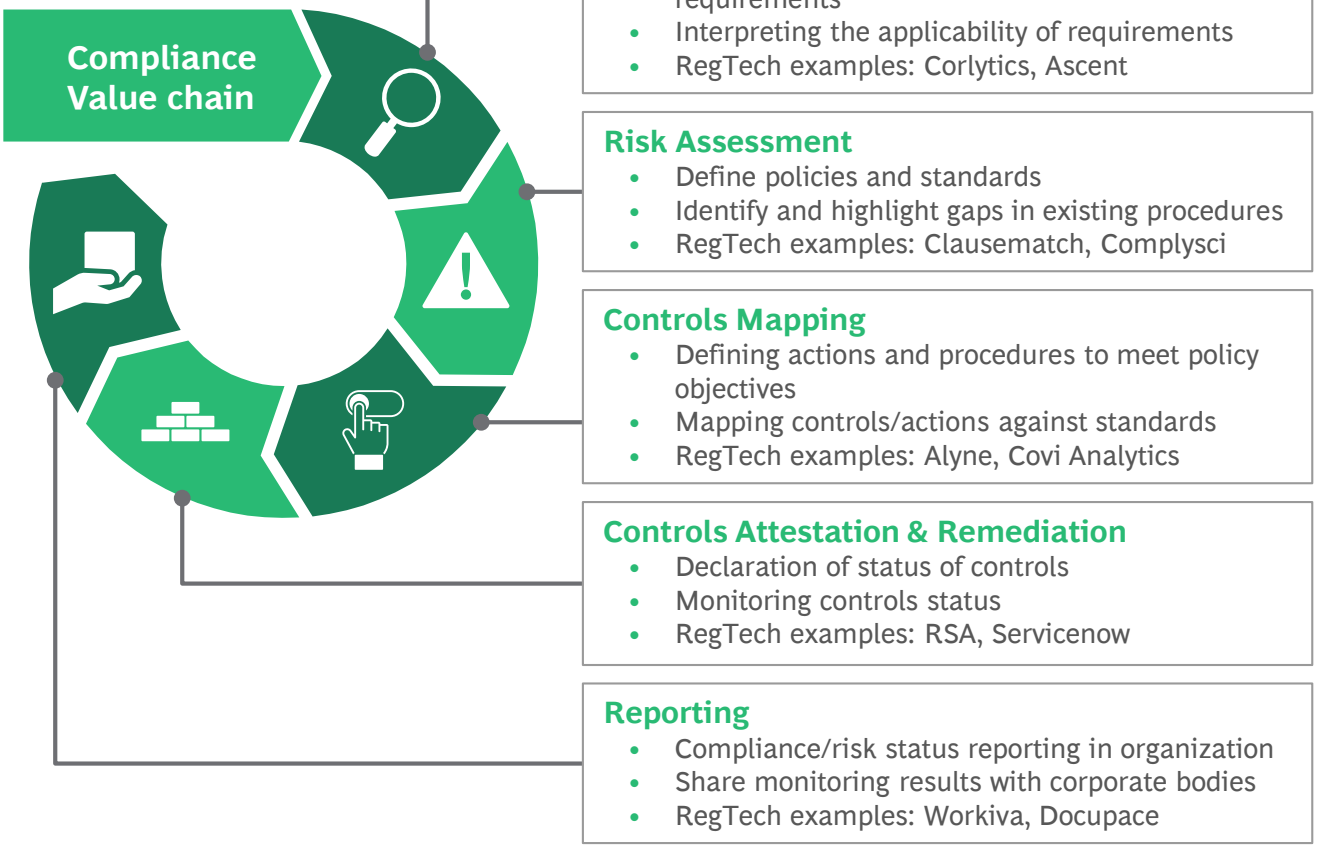
Source: Expand Research

Cybersecurity implications – what should Financial Institutions do?

At the time of writing, COVID-19 vaccines are being administered, while much of the world are still in the midst of national lockdowns. Financial Institutions must remain vigilant and find an operating model that is able to adapt rapidly to ever-changing circumstances. There are two clear implications that follow.

12. https://www.apra.gov.au/a-joint-letter-from-apra-and-asic-on-impact-of-covid-19; https://www.mas.gov.sg/news/media-releases/2020/fraudulent-phone-scams-impersonating-mas-or-bank-staff

Exhibit 9 - Compliance value chain

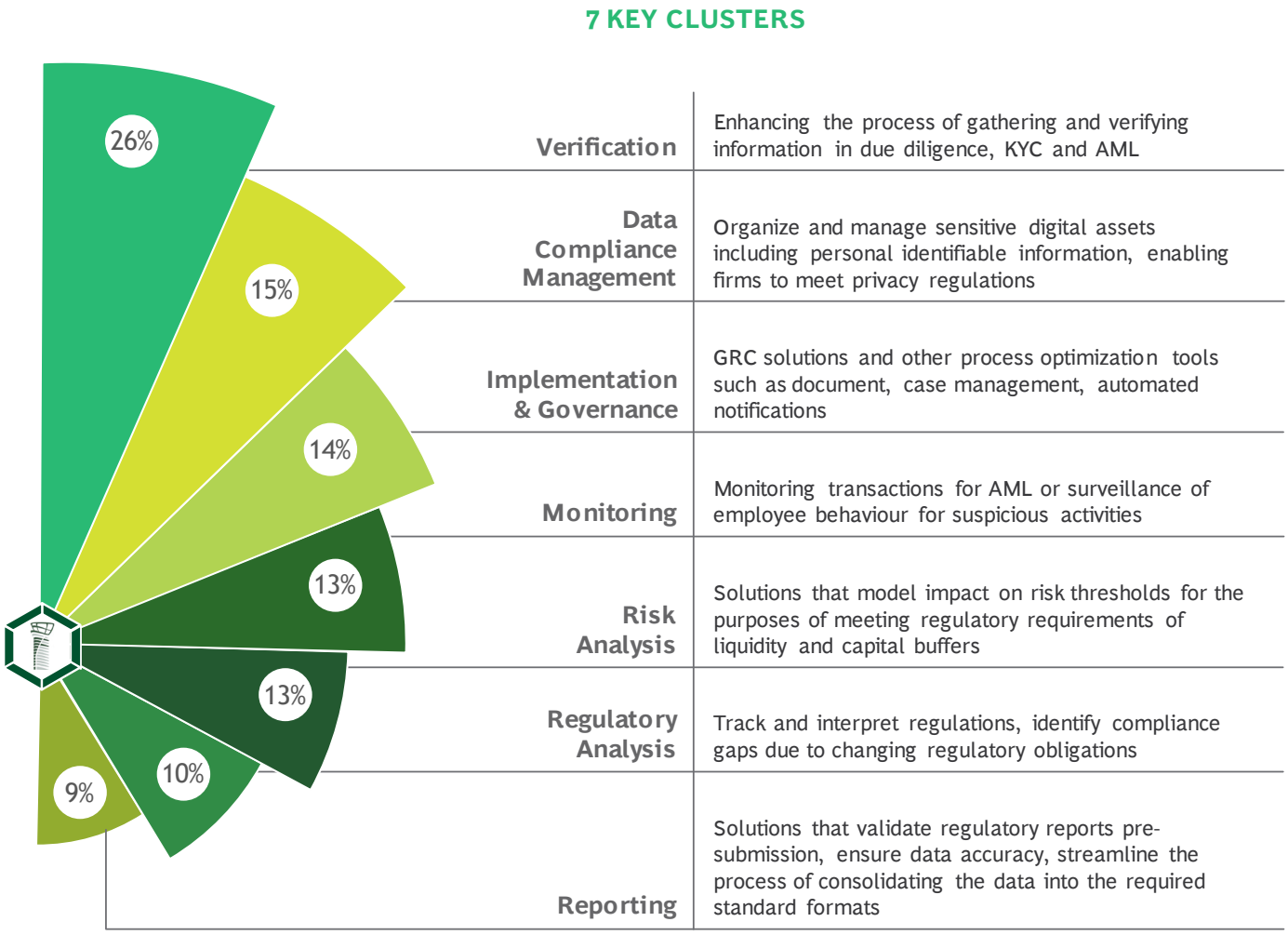


Source: BCG Expand FinTech Control Tower

First, COVID-19 has undoubtedly accelerated the path toward digitization. As remote working stabilizes into the new hybrid working model, regulators are increasingly emphasizing the benefits of RegTech solutions, a signal to financial institutions to rethink their compliance processes.[13] The opportunity is ripe for management stakeholders to relook at the productivity gains that can be gained from adopting RegTech tools.[14]

13. https://www.mas.gov.sg/news/media-releases/2020/40-innovative-solutions-shortlisted-for-mas-fintech-awards
14. https://www.bcg.com/en-au/publications/2020/australia-global-regtech-hub-poised-for-growth

Exhibit 10 - Seven key clusters of RegTech



Source: BCG Expand FinTech Control Tower

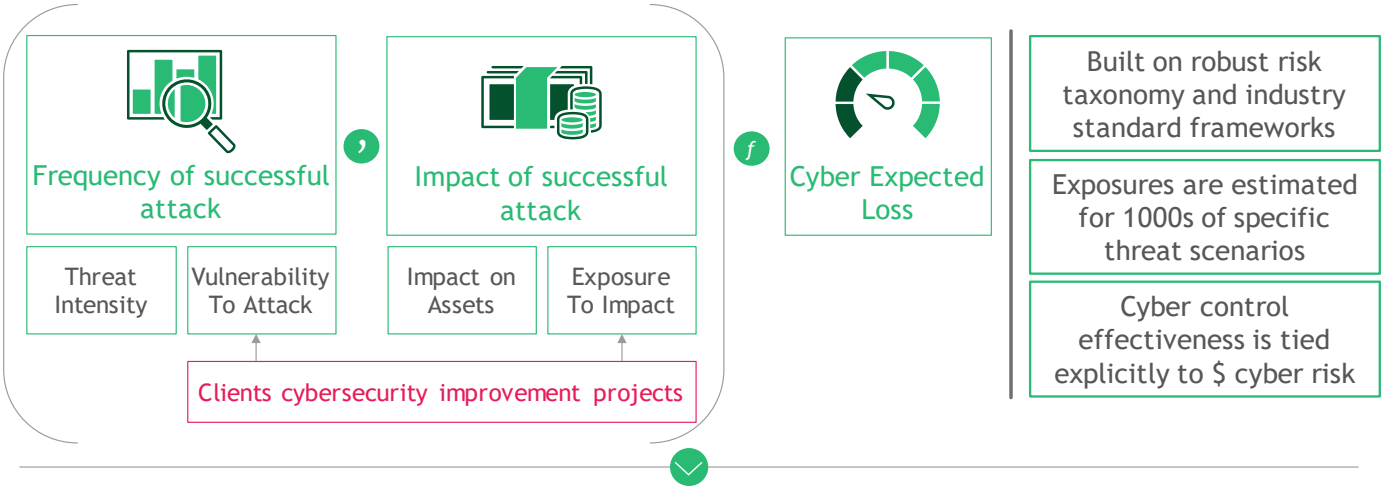
In line with these efforts, BCG Expand's Fintech Control Tower developed a comprehensive taxonomy of RegTech segments that helps organizations better understand the landscape and which RegTech product offerings answer to specific segments in the governance, risk & compliance (GRC) value chain. The largest majority of1 growing RegTech companies was identified to be in the Verification cluster, which aims to optimize outdated ways of information gathering and validation for KYC and AML. Time and effort from manual compliance processes can be reduced, and it would be prudent for financial institutions to capitalize on these efficiency improvements and achieve better risk management.

Cybersecurity

Second, even though the cybersecurity agenda is of paramount importance, organizations continue to face challenges in justifying and quantifying the return on their cybersecurity investments. Business leaders are well aware of the importance of cybersecurity, yet knowing where to start is another thing. As the cybersecurity project lists keep growing, budget allocated for cybersecurity is rarely enough to cover all projects. Analyzing project effectiveness becomes imperative to maximize the dollar value of each project. To address this pressing need, BCG developed Cyber Doppler: a methodology and software tool designed to simplify and quantify risk-based cyber project optimization. It offers three primary benefits:

- It reduces time and effort. Cyber Doppler uses easily understood, dollar-value terms to rapidly prioritize cyber risk and cyber investment.
- It justifies investment value. The approach reveals the levels of risk-exposure reduction associated with each potential cyber investment and investment strategy.
- It maximizes the value of every dollar. Leaders become equipped to allocate cyber investment to areas most in need, through control sensitivity analysis and portfolio optimization.

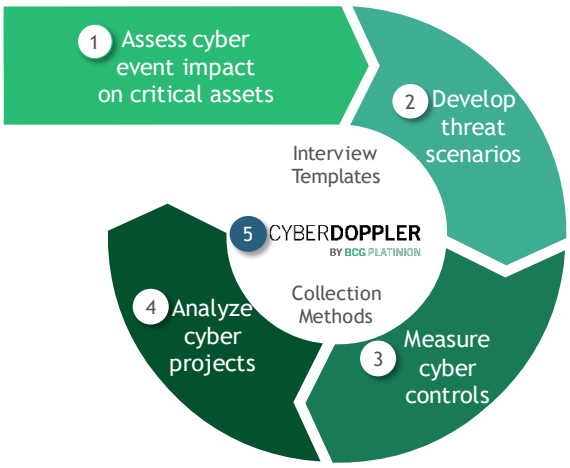
Exhibit 11 - Cyber Doppler allows clients to estimate the expected loss from cyber attacks and the impact of cybersecurity improvement projects



Estimating cyber expected loss with & without projects enables us to estimate risk reduction per project and construct a prioritized project portfolio

Exhibit 12 - BCG's approach combines the Cyber Doppler software tool, with a systematic methodology & an expert team that brings range of industry-leading skill sets

BCG's approach follows a systematic methodology to collect data & develop expert estimates…



Each data input (1-4) can be BCG-developed or client-provided (saving time & effort)

…lead by an interdisciplinary team of experts armed with skills across key areas of CRQ

Business Strategists with expert knowledge of each client industry, business ecosystem, & mode of operation

1

Cyber experts well-versed in cyber assessments, attack methodologies, & asset-centric threat modeling

2 3 4

Risk modelers experienced in mathematical & statistical modeling techniques

5

Chief information security officers (CISOs') must rethink their strategies and ensure that cyber investment is effectively optimized towards protection of high-risk assets.

Towards that end, firms require a more robust and systematic process to optimize their cyber investment strategies.

About the Authors

Pauline Wray is the Global lead of the BCG Expand FinTech Control Tower, and the Head of BCG Expand in Asia. You can reach her at pauline.wray@expandresearch.com

Maneet Ahuja is a Lead Analyst in the Singapore office of BCG Expand, and heads the IT Regulatory Risk Working Group. You can reach him at maneet.ahuja@expandresearch.com

Alain Schneuwly is BCG's Cybersecurity and Engineering lead in APAC. You can reach him at schneuwly.alain@bcg.com

Donovan Choy is an Analyst in BCG Expand's IT Regulatory Risk Working Group. You can reach him at donovan.choy@expandresearch.com

Sugar Chan is a BCG's Cybersecurity senior consultant. You can reach her at chan.sugar@bcg.com

About the IT Regulatory Risk Working Group

The data in this white paper is collected through Expand Research's IT Regulatory Risk Working Group (TRWG) platform. These interviews were conducted with a total of 14 international banks over the period of February to December 2020.

The TRWG is a research platform that assists global and regional financial institutions in navigating the complexity of the financial services regulatory landscape in Asia-Pacific. The platform provides a horizon scanning of regulations in the region and enables member participants to engage an industry peer group on key thematic subjects within the area of technology risk, exchanging industry experience and performance metrics on the different approaches of technology regulatory risk compliance.

The TRWG holds regular roundtables among IT risk regional heads of international banks. Topics are member-driven and agreed ahead of schedule. Sessions are held under Chatham House (Vegas) rules, no comments or discussion topics are made public nor are they attributable. Member banks also have the opportunity to field specific and customized poll questions to their peers, allowing for quick insights in between session meetings.

For Further Contact

For more details, please contact the authors.

bcg.com