The Declaration seeks to address one of the most pressing global issues of our time: Empower digitization, e-commerce, and innovation, while ensuring a free, open, and safe Internet.

From Security to Resilience: Taking Cyber from the Realm of the IT Experts Into the World of Holistic Risk Management and Making It a Global Public Good

Peter Sullivan Charlotte Branfield

Earlier this year, Benoît Cœuré, Chair of the Committee on Payments and Market Infrastructures (CPMI) and Member of the Executive Board of the European Central Bank (ECB), spoke of "cyber resilience as a global public good." His statement is a timely call to action, and helps elevate cyber from the world of IT experts to the wider context of economic, market, and enterprise risk management.

Cyber resilience enables us to foster financial inclusion and innovation while protecting consumers and their data. It is a critical part of the private and public sectors' shared responsibility in ensuring the financial sector's safety and soundness – a prerequisite for sustainable economic growth and social development.

This motivated Citi to become an Official Partner of Commonwealth Cyber Declaration – the world's largest intergovernmental agreement on promoting cyber resilience, across all sectors and members of the Commonwealth. The Declaration seeks to address one of the most pressing global issues of our time: Empower digitization, e-commerce, and innovation, while ensuring a free, open, and safe Internet.

On 2 July 2019, in support of the Commonwealth Cyber Declaration, Citi ran simultaneously, a multi-country, strategic-level pilot exercise lasting four hours across six African countries, in partnership with Immersive Labs, the IMF, World Bank. Participants included central banks, domestic information sharing organizations, the critical local banks, mobile money service providers, stock exchanges, clearing houses, and telecommunication firms.

The strategic nature of the exercise, focusing on fictitious global and local banks impacted by malware, explored the decisions leaders would need to consider, including market dependencies, connections, communication and escalation protocol, as well as the impact to the international and domestic payment flows.

The mix of public sector and C-suite (CEO, CFO, CRO, CIO) along with banking and public affairs heads enabled strategic conversations with wider perspectives, whilst remaining anchored in reality. These diverse views took cyber out of the domain of information security and made it a business, financial sector and real economy issue. By making it more relevant and meaningful, these types of exercises help evidence why C-Suite should care and not just delegate to the tech teams.

Cyber is a Business, not Tech, Issue

The Internet and access to data allow small- and medium-sized companies to scale globally from day one. According to Forrester,[1] global cross-border B2C e-commerce will reach US$ 627 billion by 2022, having more than doubled over just five years. This highlights how the digital economy is a key driver of growth and development across the world — with Huawei and Oxford Economics estimating that the digital economy will account for 24.3% of global GDP by 2020, growing at 2.5 times the pace of the overall global economic growth.

Cyber and the new concept of Operational Resilience are fundamental to enabling business in today's interconnected, dynamic, and technology-based market. Rapidly increasing digitization is creating new risks and amplifying existing risks. It increases technological interdependences, configuring new tech to decommissioning legacy tech, and factoring in new risks into traditional activities, such as mergers and acquisitions.

Historically, securing the payment channels has been the regulators' and industry's focus. However, focusing on payment to the right beneficiary on a timely basis is equally as important. Security of payment channels requires the same attention as does the need to develop competitive and effective platforms. Without the "pipes" of the financial system being resilient, the capital flows fueling economic development could be impaired.

Further, countries and firms perceived to have weak cyber resilience may see a decrease in foreign direct investment or access to capital, with low cyber scores in future credit ratings[2] negatively impacting access to finance. On top of this, a firm with weak cyber security can have knock-on effects on its whole sector, creating negative impacts on the wider industry or economy's performance and stability.

This directly affects other areas — poor cyber resilience impacts the available investment, resource, and deployment capabilities to deliver on the UN Sustainable Development Goals and other critical public sector initiatives.

However, the "cyber" problem is only forecasted to get worse. The Accenture & Ponemon's 2019 Cost of Cybercrime Study highlights that the over the last five years the average cost of cybercrime for an organization increased 72% to US$13.0 million. Another Accenture report[3] estimates that in the private sector, over the next five years, firms risk losing an estimated US$5.2 trillion in value creation opportunities from the digital economy to cyber security attacks.

If cyber resilience awareness, culture, and collaboration are rapidly improved over the coming years, the cost of controls and value at risk would decrease. By better understanding areas or weakness, there could be more efficient deployment of resources across both public and private sectors.

Public-Private Partnership

To be effective, the cyber public-private partnership "collective defense" model will require deeper cross-sector partnerships in a coordinated manner to reduce risk.

Whilst great progress has been made over the years coordinating information sharing, there is an urgent need to evolve the model, so that it goes beyond "sharing" to "coordinating" risk management actions based on the shared information. To improve cyber resilience, central banks and other public sector bodies need to come together to drive this collaborative risk management strategy development.

[1] https://go.forrester.com/press-newsroom/cross-border-ecommerce-will-reach-627-billion-by-2022/

[2] For example, the partnership between S&P Global Ratings and Guidewire Cyence Risk Analytics announced in 2018, following a warning in 2015 from S&P that it would downgrade credit ratings for banks with weak cyber security, even if they hadn't been breached. Moody's emphasized the threat of cyber risk in 2015 , and, similar to S&P, also announced in 2018 that it would evaluate organizations on their risk of a major impact from a cyber-attack. https://www.businesswire.com/news/home/20180216005674/en/SP-Global-Ratings360%E2%84%A2-Include-Cyber-Risk-Insights; https://www.insurancejournal.com/news/international/2015/06/10/371100.htm; http://www.maalot.co.il/publications/OAC20150708094842.pdf; https://www.moodys.com/research/Moodys-Threat-of-cyber-risk-is-of-growing-importance-to--PR_339656; https://www.cnbc.com/2018/11/12/moodys-to-build-business-hacking-risk-into-credit-ratings.html.

[3] Securing the digital economy, Accenture. https://www.accenture.com/us-en/insights/cybersecurity/reinventing-the-internet-digital-economy

To achieve this, today's public-private partnerships need to evolve from being seen as traditional IT tactical and operational information sharing or business continuity "circles of trust" to true risk management groups focused on underlying services and functions. Evolving cyber resilience in this way would not only make it more inclusive and better connected with the real economy, but also support cyber capacity building and collective strength of the financial ecosystem.

Going further, tying cyber risks to business impacts would help embed resilience in product development and daily operations (e.g., a better Secure Development Lifecycle approach that would significantly improve organizations' abilities to innovate faster while operating with lower overhead costs and fewer errors). This is increasingly important for the financial sector participants, as organizations move to the Cloud, and into a world of real time payments, real time liquidity and global concentration "engines."

In essence, the cyber collective defense model needs to evolve into an effective enterprise-wide risk-management approach where government, central banks, and industry work side by side to address and reduce risk.

This not only reduces risk; it decreases the likelihood of inefficient investment in resilience . From a development perspective, this collaborative risk management at country and sector levels would create stronger links between cyber resilience, capacity building and concessional and philanthropic funding.

It will require hard work and creativity; professionals from across firms' revenue and non-revenue generating teams will need to proactively share expertise to make cyber relatable and understood in the context of their firm's business growth and risk appetites. And we need to do this across sectors too, with the public sector.

Strategic exercises at the level of Central Bank Governor and Deputy Governor, Minister, and C-Suite would be a first step in providing a true holistic understanding of cyber risk and current state of resilience. Gamified, online interactive tools, could be leveraged in these events to anonymously gather data on decision making, and speed and certainty of response, enabling practical capacity building with credible thematic and repeatable benchmarks. These could in turn, be integrated into rankings such as the Worldwide Governance Indicators (WGI).

Strategic Cyber Exercising

For many years, firms have been encouraged to conduct internal exercises (or tabletops, war-games, simulations). Strategic industry-wide cyber crisis management exercises are crucial to achieving the strategic collective risk management model of public-private partnerships.

The critical point here is that any strategic-level public-private exercises must be kept small to enable the institutions to debate and discuss the actions they would take and why. Whilst large sector exercises, such as those run by FS-ISAC and FSARC, are important to strengthening security, they include such a large range of people and different organizations that discussion is not possible. They also rely on participants playing "using" their firms' capabilities – this also precludes group discussion as few firms today are willing to openly share what capabilities they do or don't have.

Small, strategic level exercises that enable scenario analysis and discussion can help institutions understand potential risks, how these may transmit, where investments need to be made, and how best to respond when systems are breached.

On 2 July 2019, in support of the Commonwealth Cyber Declaration, Citi ran simultaneously a multi-country, strategic-level pilot exercise lasting four hours across six African countries. Citi conducted this in partnership with Immersive Labs, the IMF, World Bank. The exercise included SWIFT, domestic information sharing organizations, such as SABRIC, and banking associations, as well as Deputy Central Bank Governors and ICT regulators per country. Firms critical to each country's respective financial sector from the top five local banks to mobile money service providers, stock exchanges, clearing houses, RTGS platforms, and telecommunication companies were included.

The scenario involved fictitious global and local banks impacted by a malware which paralyzed their operations. As the scenario unfolded, it became evident that the driver behind the coordinated cyber-attack was payment manipulation.

Each country's participants came together in a single location, and for the first half of the exercise, they took part in the scenario within the country, before joining together on a regional video call to discuss the cross-border elements. Responses to the scenario were multiple-choice: each participant could select an answer directly in the online platform, with each country's participants required to come to agreement

on a single group "country" answer – and each option was designed to impact to Funding & Liquidity, Share Price, Market Confidence and Reputation, illustrating the balancing of risks and impacts in crisis scenarios.

The pilot exercise also highlighted the power of creating a safe, learning environment. By leveraging Immersive Lab's interactive online (web-based) platform at the event, the participants could directly and anonymously engage with the scenario whilst also benefiting from a structured discussion, with the multiple-choice providing optionality, driving debate within the country locations. By doing this, and using fictitious banks, participants were better enabled to engage in discussion, with no barriers to engagement, nor need to share details of their own cyber security programs and subsequent risk of inference that others were worse/better than the rest.

Key themes from Citi's Africa Exercise

- **Preparation is Key:**
  - There is a need for a proper recovery strategy framework with playbooks for each sector and at a country-level. These playbooks should include escalation procedures, external communication and information sharing arrangements, roles and responsibilities, and clearly defined roles for the Bankers' Association, Communications Regulator, and Central Bank. This information should be captured as appropriate within the national/financial crisis management frameworks.
  - In addition to a sector playbook, both the private and public sector require their own broad institution-specific playbooks to help guide response practices with pre-defined trigger thresholds for deployment of containment procedures and escalation protocols.
  - Banks whose revenue-generating teams signed-off/sponsored their playbooks, instead of delegating to their information security or business continuity teams, appeared to have a much better understanding of the trade-offs when making decisions.
  - Central banks had a vital role to play in connecting the banking and payments associations, as well as developing a proactive mechanism to convene industry in the event of an incident.
  - In particular, clarity was called for over who should handle media statement(s): individual banks (to manage their stakeholders and confirm they are not affected, which may see over 20 statements shared with the public, for example) or a single response from the central bank (to ensure market stability and reassure confidence in the market)?
- **Deeper Trust to Enable Information and Risk Sharing is Needed**
  - Value of information sharing was recognized; and more trust in the market is needed to progress this, which can be developed through collective exercising.
  - Need to have a mechanism to share and review emerging risks, and to perform annual risk assessments with outputs shared and included in playbooks (with exercises then validating these).
  - Many noted that it was important to keep a clear distinction between threat intelligence/information sharing for early warning purposes vs. for regulatory notifications/reporting requirements.

Key themes from Citi's Africa Exercise *(continued)*

- **Decision-Making for All Needs Work**
  - Responses were sometimes slow and uncertain. Confidence and decision-making ability started to really break down as the event became cross-border and cross-sectoral.
  - At a domestic level, participants recognized much value in identifying a single umbrella organization to help coordinate responses by sharing threat intelligence, responses, and changes in the market and risk to the market.
  - More discussions were called for regarding what triggers should exist regarding central bank intervention in a cyber event.
  - There was a recognized need for a "rapid-response unit" at strategic CEO and CRO levels (i.e., how do they all get on a call and ensure proper understanding of business impacts?).
- **Systemic risk**
  - The participants were in agreement that cyber related risks/events could easily escalate into a full/system wide crisis if not well managed by all the relevant stakeholders in a quick and timely manner (as a result of panic, reputation damage, or loss of confidence in the financial system).
  - Tension/fine balance between taking action to save your firm (but risk market stability) vs. taking action to protect market stability (risking individual stability); need more discussion on individual vs collective market actions in a cyber event – and there is a need for clear regulatory guidance on this and their expectations (at a multi-country level).
  - Scope of impact could extend to the capital market and impact settlement done via the financial market. Given a cyber event is likely a multiple day event, public and private sectors need to consider the T+2 impacts.
  - Views that existing liquidity back-stop arrangement and similar initiatives on reaching out to a pre-agreed partner bank in case of a need for liquidity or injection of funds will not work in a cyber event, as they were not designed with a cyber-attack in mind.
  - The longer term trade-offs require further discussion and exploration from a systemic perspective and if short-term containment had been prioritized (possibly appropriately).
  - Clarity is required on who provides assurance to the market that the systems of the impacted bank(s) are operational with integrity – how do you know you have recovered from a cyber-event? Who provides the attestation? What do you trust/take comfort from? Timeframe for this can be months.

Citi's pilot exercise showed the continued need for financial sectors and countries to come together, find a common ground, and build cyber resilience. Through improving interconnectivity among industry players and public sector, exercises are a practical way to highlight the need for a proper recovery strategy framework and playbooks for each sector and at a country- and multi-country levels.

As the global architecture of cyber resilience (and Operational Resilience) regulation evolves over the next two to five years, cross-border collaboration and public-private sector partnerships will be needed more than ever to establishing robust multilateral cooperation, common cyber response and recovery frameworks, and developing scalable, outcomes-based risk-management techniques.

The role of business is fundamental, both to transition away from practices that undermine the attainment of cyber security and to proactively create solutions that solve existing cyber challenges.

No firm can gain advantage in this space; with our interconnected financial ecosystem and shared technological dependencies, we all rely on a common credibility and confidence structure. A cyber incident at one institution could have a significant impact on others. Partnerships between financial institutions and the public sector, including Central Banks, Development Banks, Ministries of Finance and Ministries of Foreign Affairs is vital.

Over the past year, there has been increased momentum and energy galvanizing the private sector to consider the role it plays in advancing cyber resilience through cyber capacity building.

More is needed.

This is well-aligned with Citi's mission and vision. Citi, as the world's global bank, has a vital role to play, including deploying services and products to address the challenges of resilience in an intentional way and supporting others to do the same. Private-sector support of the public sector, and continued public sector leadership are essential. The risk of not acting is a costly proposition with potentially detrimental consequences for the public sector sustainable development, financial inclusion and innovation agendas, and a suboptimal and diffused deployment of public sector's resources.

Peter Sullivan
Head of Africa, Citi

Charlotte Branfield
Head of Cyber Engagement, Chief Information Security Office & Enterprise Infrastructure, Citi