American Bankers Association

Building Success. Together.

Denyette DePierro
Vice President and Senior Counsel
Cybersecurity and Digital Risk
Office of Advocacy and Innovation
P 202-663-5333
ddepierr@aba.com

Monday, July 20, 2020

Financial Stability Board
Secretariat
Bank for International Settlements
Centralbahnplatz 2
CH-4002 Basel
Switzerland
CIRR@fsb.org

Submitted electronically on July 20, 2020

Re: Consultative Document: *Effective Practices for Cyber Incident Response and Recovery* (April 20, 2020)

Dear Sir or Madam:

On behalf of the United States banking sector, the American Bankers Association (ABA)[1] appreciates the opportunity to respond to the Financial Stability Board (FSB) April 2020 consultative document, *Effective Practices for Cyber Incident Response and Recovery* (CIRR) ("the Toolkit"). This response focuses on the Toolkit's reflection of the cybersecurity, business continuity practices, and operations of community and midsize banking sector.[2]

The Toolkit is presented as non-technical review of 7 cybersecurity categories and their underlying 46 effective practices. It offers a comprehensive review of the many aspects of cybersecurity that may be found in a functioning, well-performing approach to incident response and recovery. In addition to the CIRR review, the FSB further asks how the 2020 SARS-CoV-2 global pandemic is causing institutions to reevaluate their existing CIRR and business continuity planning.

[1] The American Bankers Association is the voice of the nation's $20.3 trillion banking industry, which is composed of small, regional and large banks that together employ more than 2 million people, safeguard $15.8 trillion in deposits and extend nearly $11 trillion in loans.

[2] This letter incorporates by reference the companion joint trade association letter signed by the ABA and the Bank Policy Institute (BPI) submitted July 20, 2020. This letter focuses on the response of a specific subsector of the US financial services industry—community and midsize banks.

Although not easily defined, a community-focused midsize financial institution in the US market is usually described as having less than $50B USD in assets[3] and operating within a defined footprint, which may be regional, covering several states, or a single municipality. On average, a community bank has approximately $265M USD in assets, fewer than 100 employees, and a distinct footprint. When considering the impact of a wide ranging document, such as the FSB's CIRR consultation, we must carefully consider how an institution of this size, holding these resources and personnel, could efficiently adapt and adopt the CIRR Toolkit to fit their risk and complexity.

On behalf of ABA's community and midsize bank members, this letter suggests 7 recommendations to enhance the Toolkit's relevance and reflection of this segment of the financial services industry:

1. Clearly articulate the purpose, intended use, and audience;
2. Include examples, cross references, and samples to aid readability and encourage the global uptake and development of working models and approaches;
3. Refine CIRR as incident agnostic focusing on robust capacity, resiliency, and flexibility;
4. Encourage, recognize, and validate private sector approaches to CIRR;
5. Affirm reliance on harmonized cybersecurity principles aligned with international cybersecurity standards;
6. Reiterate and support a firm's cybersecurity posture as commiserate with complexity and risk; and
7. Acknowledge that a fundamentally adept and adaptive CIRR posture allows banks to play an important public leadership role when an incident impacts customers and community.

[3] The $50B USD asset threshold was first defined in the Dodd–Frank Wall Street Reform and Consumer Protection Act in 2010 as the asset size designating a financial services company as systemically important and subject to enhanced supervision. For supervisory purposes, the assets threshold for systemically important institutions was amended in 2018 to $250B USD, but the $50B asset threshold continues to function as a soft indicator of a community-based institution. Readers should note that asset size does not solely define a community institution; other elements such as business model, operations, and ownership structure also should be considered.

Articulate the purpose, intended use, and audience.
In order to help define the FSB's intended use for the Toolkit and address latent industry concern that a principles-based survey of CIRR could lead to prescriptive regulations, it would be helpful to clearly articulate in the opening paragraphs that this is a toolkit of *options* that could be considered within the design of a functioning CIRR. The Toolkit should further illustrate that the CIRR of a particular institution should be crafted according to the maturity and risk profile of the firm and not a "one-size-fits-all" approach. Moreover, it would be unusual, if not highly unlikely for any one firm to adopt all 7 categories and every 46 effective practices described in the Toolkit. Rather, a secure, functioning, well-performing CIRR may include some or many of the effective practices, but also may include aspects not described in the Toolkit. Supervisors and senior leadership reading the Toolkit should be encouraged to consider the need to build capacity and resiliency within their institutions while also encouraging flexible agile response to an incident—or overlapping incidents. This requires moving beyond a CIRR checklist to embrace creative problem solving within a challenging, dynamic environment.

The simple, non-technical language of the Toolkit reveals that the intended audience is not cybersecurity or technology professionals, but rather senior management, board of directors, or other compliance, risk, and legal professionals that interface with cybersecurity, but do not implement or manage the institution's cybersecurity program. If this is correct, it would be helpful to identify the intended audience in the Toolkit's introduction and explain why the FSB considers the Toolkit valuable for a non-technical audience. A statement from the FSB would bring further clarity to the use and underlying intent of the Toolkit as well result in non-technical staff reading the Toolkit and relying on it as a resource and reference guide.

Include examples, cross references, and samples to aid readability and encourage the global uptake and development of working models and approaches
The descriptions of the 46 effective practices, although helpful, can be vague and difficult to decipher. The readability and comprehension of the Toolkit would be aided by including examples, references, and samples within footnotes, internal hyperlinks, or an appendix. Including references to working models and approaches from a cross-section of jurisdictions that demonstrate the identified effective practices would enhance the usefulness of the Toolkit as a CIRR resource. For example, effective practice #10, *Plans and Playbooks*, could include references to the Financial Services Information Sharing and Analysis Center (FS-ISAC) *All Hazards Framework*[4] and the ABA/FS-ISAC collaboration, *State Incident Response Playbook*.[5] As a sample playbook, these offer tangible demonstrations of the identified effective practice while offering a model for download, review, and potential use or adaption in other jurisdictions.

[4] www.fsisac.com/hubfs/Resources/FSISAC_AllHazardsFramework_TLPWhite.pdf (Oct 15, 2019).
[5] The American Bankers Association, the ABA-State Association Alliance, the Financial Services Information Sharing and Analysis Center (FS-ISAC) and critical infrastructure partners developed an all-hazards state and regional crisis Incident Response Playbook for each of the 50 US states. The Playbook guides how banks located in each state will respond during a crisis event, how activities will be coordinated, and how information will be shared to achieve resiliency in the financial sector. Each of the 50 state-specific playbooks include state and federal agency contact information. www.aba.com/news-research/references-guides/incident-response-playbook

Refine CIRR as incident agnostic focusing on capacity, resiliency, and flexibility.
The pandemic experience has reiterated for many community and midsize banks that robust response and recovery is incident agnostic, and rarely incident specific. Many of the lessons learned from prior incidents that enable banks to respond to the rapid deployment of a remote workforce in a pandemic were prior natural disasters, severe weather, wild fires, and floods. In the midst of the pandemic, banks also realized that they and their customers were faced with increased fraud attempts and cyber risk while working to secure, train, communicate, and deploy hardware and virtual platforms to employees working from home, sometimes for the first time. Concurrently, banks needed to address the health and well-being of their employees and customers at the same time as essential employees were becoming ill with CoViD-19.

The shared goal of supervisors and industry as reflected in the Toolkit is a resilient global financial services sector with the capacity and capability to respond and recover from overlapping and concurrent incidents. This requires considering how CIRR fits into incident response across an array of possible incidences or intersecting incidents, and the need to build cross-sector resiliency. A Toolkit focusing on capacity, flexibility, and resiliency on a continuum, rather than a fixed before/during/after timeline, is more reflective of incident risk and occurrence and aligns with building the resiliency and capacity of the sector.

Encourage, recognize, and validate private sector approaches to CIRR.
In recent years, the US financial services sector has witnessed the development of several novel CIRR solutions. These solutions, created and often collaboratively managed within the private sector, enhance the collective security and resiliency of the broader financial services marketplace. ABA suggests these approaches be incorporated into the Toolkit as identified examples of effective practices. Concurrently, FSB may consider the important role the private sector plays in identifying solutions and encourage continuing CIRR innovation by recognizing and accepting these effective private sector practices as credible, substantive, and valid. Of these private sector innovations, there are 5 solutions of particular importance to community and midsize banks:

1. Financial Services Sector Cybersecurity Profile assessment tool,
2. Cyber insurance,
3. Collaborative data vaulting and recovery of Sheltered Harbor,
4. Enhanced domain security embodied in the sector's acquisition and management of the .bank and .insurance domains as an anti-phishing and security measure; and
5. Collaborative threat and intelligence sharing platforms that include training and policy development, such as Financial Services Information Sharing and Analysis Center (FS-ISAC) and Financial Service Sector Coordination Council (FSSCC).

Financial Services Sector Cybersecurity Profile Assessment

Known as the Financial Services Profile (FSP) in Europe, and the Profile in the US, the Cyber Risk Institute's (CRI) Cybersecurity Profile[6] was a collaborative effort of 150 financial firms and more than 300 bank representatives over several years. The result is a unified harmonized approach to cyber security assessments that can be used by the smallest and the largest financial services firms: banks, securities, and insurance. The CRI Cybersecurity Profile is recognized as a global cyber tool and convergence instrument bringing together a catalogue of global security standards, regulations, and legal framework requirements.

Cyber Insurance

As an important risk transfer option for small and midsize banks, cybersecurity insurance is a component of efficient CIRR practices for some institutions not mentioned in the Toolkit.[7]

Sheltered Harbor

The concept for Sheltered Harbor[8] arose from a sector-sponsored cybersecurity tabletop exercise that identified a security gap in the recovery and restoration of data in the aftermath of a severe cybersecurity incident. Responding to that risk, an industry-led collaboration of financial institutions, core processors, national trade associations, and third party service providers created a not-for-profit company to develop a resilient data vaulting process.

Domain security and phishing mitigation: .bank and .insurance

In response to the creation of new financial services domains and industry concerns that .bank and .insurance would be easily exploited for phishing and social engineering enabled fraud, a coalition of global banks, insurance companies and financial services trade associations[9] were granted the right to operate these domains.

An observable trend during the 2020 pandemic when coupled with the banking sector's central role in facilitating economic stimulus and disaster loan programs was an increase in phishing attempts against bank customers and financial services firms. The enhanced domain security built into .bank and .insurance is an effective fraud mitigation and resiliency practice for institutions of all sizes that can be deployed across any existing domain. Domain security is a component of risk mitigation of proven value during the pandemic that is not identified as an effective practice in the Toolkit.

---

[6] www.cyberriskinstitute.org

[7] "As with any insurance coverage, cyber insurance does not diminish the importance of a sound control environment. Rather, cyber insurance may be a component of a broader risk management strategy that includes identifying, measuring, mitigating, and monitoring cyber risk exposure. US Federal Financial Institutions Examination Council (FFIEC), *Joint Statement on Cyber Insurance and Its Potential Role in Risk Management* (April 10, 2018). www.ffiec.gov/press/pdf/FFIEC%20Joint%20Statement%20Cyber%20Insurance%20FINAL.pdf

[8] www.shelteredharbor.org

[9] This founding coalition now operates as fTLD Registry Services, LLC. (www.ftld.com) All users of the domains are verified to be legitimate financial services companies and comply with strict compliance and security requirements. As a result, customers know that users of these domains are trusted, verified, and secure.

FS-ISAC and FSSCC

FS-ISAC is a private-sector industry consortium with a global reach dedicated to reducing cyber risk in the global financial system offering a platform to exchange intel on threat and risks within a peer-to-peer network.[10] It shares a close affiliation with FSSCC which often acts as liaison and collaboration hub among the financial services industry, federal financial services supervisors, and the federal government.[11] For many community and midsize banks, their primary resource for threat intelligence and education is the FS-ISAC network and peer groups. FS-ISAC and FSSCC are effective models of intel sharing and private/public sector collaboration that could be used as a working model of an effective practice in the Toolkit.

Affirm reliance on harmonized cybersecurity principles aligned with international cybersecurity standards.

A central tenant of the FSB's work on cybersecurity and the foundation of the cybersecurity lexicon was global harmonization of terminology and principles that reflect internationally recognized cybersecurity standards, such as:

1. National Institute of Science and Technology Cyber Security Framework (NIST CSF),
2. International Organization for Standardization (ISO),
3. Bank for International Settlements Committee on Payments and Market Infrastructure and International Organization of Securities Commissions (CPMI-IOSCO), and
4. ISACA's Control Objectives for Information and Related Technologies (COBIT).

The recognition and alignment with common standards should also encourage institutions to use their preferred framework, or frameworks, that best guide the firm's cybersecurity, and enable a more resilient and responsive financial services sector. Among US financial companies, there is growing reliance on the CRI Cyber Profile, particularly among community and midsize banks, as a compendium of standards that maps among the standards while converging and harmonizing local, national, and global approaches to cybersecurity.

[10] FS-ISAC has approximately 15,000 users from 7000 banks in 70 jurisdictions. www.fsisac.com

[11] FSSCC's "70 members consist of financial trade associations, financial utilities, and the most critical financial firms. FSSCC partners with the public sector on policy issues concerning the resilience of the sector." www.fsscc.org

Significant Support for the CRI Cyber Profile Among Community and Midsize Banks

In response to industry's growing interest in the CRI Cyber Profile, ABA hosts two peer groups for Profile users: one group for community and midsize banks (Tier 3 and 4 institutions), and one group for regional, national, and global financial companies (Tier 1 and 2 institutions).[12] The community and midsize bank peer group has more than 170 active members and continues to increase in number. Similar to the Tier 1 and 2 institutions, this peer group cites the utility of the Profile as a convergence document of state and national rules grounded in commonly used internationally recognized standards.

In an informal survey of 126 state bank supervisors in December 2019, 47.8% of the participants reported seeing the CRI Cyber Profile used in the field and nearly ½ of those respondents had seen it used at more than one institution.[13] When asked about the asset size of the CRI Cyber Profile user banks they observed, the supervisory staff reported:

- 36.1 % were banks under $500M USD in assets,
- 38.8% were banks with assets of $500M - $1B USD,
- 16.6% were banks with assets of $1B – $10B USD, and
- 8.3% were banks with more and $10B USD in assets.

Given that nearly 75% of observed bank users were under $1B USD in assets, the utility of the CRI Cyber Profile for even the smallest institutions is evident. The Toolkit offers an opportunity to acknowledge the CRI Cyber Profile as a singular approach to cyber security assessments that can be used by institutions of all sizes and complexity in any jurisdiction, and can be tailored according to the individual institution's risk characteristics.[14]

[12] The ABA Profile Peer Group –Tier 1 and 2 has elected to accept Tier 1 and 2 financial services companies, including insurance companies and securities firms.

[13] Online survey conducted by ABA on December 11, 2019 of 126 state bank supervisors attending a remote seminar on the CRI Cyber Profile cohosted by ABA, CRI, and the Conference of State Bank Supervisors (CSBS).

[14]The CRI Cyber Profile begins its cyber assessment with a 9-question survey that identifies the institution's risk based on operational characteristics, not asset size. Institutions are then categorized as Tier 1 (highest risk), 2, 3, or 4 (lowest risk) and the number of assessment questions is tailored to the institution: Tier 1 = 277 assessment questions, while Tier 4 = 136 assessment questions.

Reiterate and support a firm's cybersecurity posture as commiserate with complexity, resources, and risk.
Only some of the Toolkit's 46 effective practices are further refined in the text as needing to be tailored according to a firm's risk and complexity. Analogous to a clear statement of the FSB's intended use and audience, the Toolkit would also benefit from a statement embracing an overarching rule of proportionality. This statement should appear at the beginning of the document to encompass all 46 effective practices within a risk-based approach.

There are several areas in the Toolkit where the language is not inclusive of smaller, less complex financial services companies and may not be perceived by community and midsize banks as applicable to their business model. This is particularly noticeable to institutions that rely on third-party services providers as an essential primary facet of the IT or CIRR team. Examples of the exclusionary language include the identified effective practices of a Media Spokesperson, under effective practice # 3, *Roles, responsibilities and accountabilities for CIRR*, the strict categories of external and internal stakeholders in listed in Box 2, *Examples of internal and external stakeholders*, and the prioritization of stakeholder interactions and communications described throughout the Preparation section.

The implication of the Toolkit's language is that primary stakeholders are internal employees, without acknowledging the multi-disciplinary approach of many smaller institutions, which largely depend on external third parties to function as primary legal counsel, crisis communications experts, core service and technology providers, IT and technology staff, and forensics and technology management, among other services. This substantial and essential reliance on third parties applies across financial services companies, including community and midsize banks, small broker dealers, and independent insurance agents.

In order to develop a cybersecurity approach inclusive of banks of all sizes and business models, the Toolkit should recognize the resources, complexity, and business models utilized by smaller institutions and how these operate in the bank and within CIRR. The language of the Toolkit could state that some institutions often rely on consultants, core processors, third party service providers, and external experts as primary stakeholders to accomplish the tasks outlined in the 46 effective practices. It could further reiterate that every bank may not integrate all 46 effective practices as is appropriate for their risk, complexity, and business model.

Acknowledge that a fundamentally adept and adaptive CIRR posture allows banks to play a public leadership role when an incident impacts a bank's customers and community. The primary role many banks play in their communities' incident response and recovery is not reflected in the Toolkit. Community and midsize banks often engage in high-touch customer service and education during an incident. This may include significant anti-fraud, business email compromise, ransomware, and cybersecurity education as well as food, water, shelter, and infrastructure. During an incident, banks are known to function as community response hubs offering meeting space, free wifi access, or a location to recharge phones and equipment from the bank's on premise emergency supplies and generators.[15] Due to their deep ties in the community, these banks often are relied upon in times of crisis to disseminate accurate information, and often, to offer direct assistance to their customers, local community, and first responders.

Good cybersecurity and CIRR practices grounded in internationally recognized standards play an essential role in allowing banks to engage as highly visible leaders and trusted community resources. Robust cybersecurity fundamentals coupled with the capacity to be resilient and agile in a crisis are essential and effective practices. The pandemic experience demonstrates the important role these characteristics played in deploying a secure and rapid response to support employees, assist customers, and aid communities in the midst of a challenging environment.

Thank you for the opportunity to respond to the Toolkit's consultative document and to participate in the series of FSB-sponsored roundtable discussions hosted in support of this important endeavor. I invite you to contact me directly with questions.

Sincerely,

Denyette DePierro
Vice President and Senior Counsel

[15] Branch locations of large financial institutions may play these roles as well.