BIS

Newsletter on cyber security

Summary of document history

Previous **version** | Previous **consultation** | This version | Subsequent **consultation** | Subsequent **version**

This version

N **BCBS** | Newsletters | 20 September 2021 | Status: **Current**

Topics:

Cyber threats and incidents, such as ransomware attacks, have emerged as a growing concern for the banking sector over the past several years, posing risks to the safety and soundness of individual banks and the stability of the financial system. Since the onset of the Covid-19 pandemic, these concerns have heightened. Remote working arrangements and increased provision of financial services using digital channels have enlarged banks' attack surfaces. This means that malicious actors, who have become increasingly sophisticated, have more points of access to banks' systems. Targeted attacks on banks' third-party service providers, including third-party software banks commonly use and intragroup entities, are also a stark reminder that cyber security measures should take into account operational dependencies on such providers. Ransomware will continue to be one of the key cyber security threats facing the banking industry. Reflecting its growing importance, cyber security is a key element of the Basel Committee's workplan, which the Group of Governors and Heads of Supervision approved earlier this year.

On 31 March 2021, the Committee issued two documents related to operational risk and operational resilience: the revised Principles for the Sound Management of Operational Risk (PSMOR) and the Principles for Operational Resilience (POR). The PSMOR were revised in part to take better account of the operational risks associated with information and communication technology, including vulnerability to cyber threats. In addition, as set forth in the POR, in today's environment a key component of banks' operational resilience (that is, a bank's ability to deliver critical operations through a disruption) is resilience to cyber incidents, including those that may arise from outsourcing arrangements. Attaining such resilience requires banks to identify and protect themselves from threats and potential failures. They must also respond and adapt to, as well as recover and learn from, disruptive events to minimise their impact on the delivery of operations, particularly critical operations.

The Committee believes that it is important for all banking authorities to encourage the institutions they oversee to adopt tools, effective practices and frameworks, including provisions for testing their efficacy, for cyber risk management that are aligned with widely accepted industry standards. Adopting such approaches will allow banks to better identify, assess, manage and mitigate their exposures to cyber risks, including those arising from third-party service providers. This will foster greater resilience to cyber threats and incidents in furtherance of the PSMOR and POR. Further, use of such cyber risk management approaches puts banks' efforts to address cyber security threats and incidents on a sound footing. In addition, the use of such approaches can facilitate supervisory oversight and help promote further alignment of supervisory assessments across jurisdictions.

The Committee in general does not endorse any particular tool, effective practice or framework, but welcomes the adoption by banks of those in use globally that align with widely accepted industry standards. The commonality of content and form across these standards demonstrates the global consensus that now exists on key cyber security principles. Available tools, effective practices and frameworks aligned with industry standards include the National Institute of Standards and Technology (NIST) Cybersecurity Framework, International Organization for Standardization (ISO) 2700x, and the Center for Internet Security Critical Security Controls. In addition, supervisors may wish to

encourage their banks to use resources such as the FSB's Cyber Incident Response and Recovery toolkit and its cyber lexicon. Many of these tools, effective practices and frameworks are publicly and freely available to banks.

The Committee believes that in the current environment banks must continually strive to improve their resilience to cyber security threats and incidents. More widespread adoption of tools, effective practices and frameworks based on widely accepted industry standards should strengthen banks' cyber security by improving fundamental elements that include effective cyber risk management, diligent cyber hygiene practices, appropriate methods for identifying and protecting against cyber threats, and enhanced response and recovery capabilities. As set forth in its workplan, the Committee will continue to monitor and assess developments in banks' cyber risk management and resilience to help safeguard the confidentiality, integrity and availability of banks' systems and data in the face of cyber threats. The Committee will take steps as needed to foster individual banks' safety and soundness and limit potential financial stability implications.

Related information

- Press release: Basel Committee calls for improved cyber resilience, reviews climate-related financial risks and discusses impact of digitalisation