NBA Nebraska Bankers Association

www.nebankers.org

Update COMPLIANCE

November 4, 2022 Vol. XXXVIII, No. 21

CYBER INCIDENT REPORTING

I. INTRODUCTION

The Financial Stability Board (FSB) has issued a set of recommendations for standardizing cyber incident reporting (CIR) among financial institutions (FI) and regulators. Cyber incidents are rapidly growing in frequency and sophistication. At the same time, the cyber threat landscape is expanding amid digital transformation, increased dependencies on third-party service providers and geopolitical tensions. Growing interconnectedness of the financial system increases the likelihood of a cyber incident at one financial institution or an incident at one of its third-party service providers having spill-over effects across borders and sectors.

II. RECOMMENDATIONS

The FSB report sets out the following recommendations to address impediments to achieving greater convergence in CIR. The recommendations aim to promote convergence among CIR frameworks, while recognizing that a one-size-fits-all approach is not feasible or preferable. Financial authorities and FIs can choose to adopt these recommendations as appropriate and relevant, consistent with their legal and regulatory framework.

1. **Establish and maintain objectives for CIR.** Financial authorities should have clearly defined objectives for incident reporting, and periodically assess and demonstrate how these objectives can be achieved in an efficient manner, both for FIs and authorities.

2. **Explore greater convergence of CIR frameworks.** Financial authorities should continue to explore ways to align their CIR regimes with other relevant authorities, on a cross-border and cross-sectoral basis, to minimize potential fragmentation and improve interoperability.

3. **Adopt common reporting formats.** Financial authorities should individually or collectively identify common data requirements, and, where appropriate, develop or adopt standardized formats for the exchange of incident reporting information.

4. **Implement phased and incremental reporting requirements.** Financial authorities should implement incremental reporting requirements in a phased manner, balancing the authority's need for timely reporting with the affected institution's primary objective of bringing the incident under control.

5. **Select incident reporting triggers.** Financial authorities should explore the benefits and implications of a range of reporting trigger options as part of the design of their CIR regime.

6. **Calibrate initial reporting windows.** Financial authorities should consider potential outcomes associated with window design or calibration used for initial reporting.

7. **Minimize interpretation risk.** Financial authorities should promote consistent understanding and minimize interpretation risk by providing an appropriate level of detail in setting reporting thresholds, including supplementing CIR guidance with examples, and engaging with FIs.

8. **Extend materiality-based triggers to include likely breaches.** Financial authorities that use materiality thresholds should explore adjusting threshold language, or use other equivalent approaches, to encourage FIs to report incidents where reporting criteria have yet to be met but are likely to be breached.

9. **Review the effectiveness of CIR processes.** Financial authorities should explore ways to review the effectiveness of FIs' CIR processes and procedures as part of their existing supervisory or regulatory engagement.

10. **Conduct ad-hoc data collection and industry engagement.** Financial authorities should explore ways to complement CIR frameworks with supervisory measures as needed and engage FIs on cyber incidents, both during and outside of live incidents.

11. **Address impediments to cross-border information sharing.** Financial authorities should explore methods for collaboratively addressing legal or confidentiality challenges relating to the exchange of CIR information on a cross-border basis.

12. **Foster mutual understanding of benefits of reporting.** Financial authorities should engage regularly with FIs to raise awareness of the value and importance of incident reporting, understand possible challenges faced by FIs and identify approaches to overcome them when warranted.

13. **Provide guidance on effective CIR communication.** Financial authorities should explore ways to develop, or foster development of, toolkits and guidelines to promote effective communication practices in cyber incident reports.

14. **Maintain response capabilities which support CIR.** FIs should continuously identify and address any gaps in their cyber incident response capabilities which directly support CIR, including incident detection, assessment and training on a continuous basis.

15. **Pool knowledge to identify related cyber events and cyber incidents.** Financial authorities and FIs should collaborate to identify and implement mechanisms to proactively share event, vulnerability and incident information amongst financial sector participants to combat situational uncertainty, and pool knowledge in collective defense of the financial sector.

16. **Protect sensitive information.** Financial authorities should implement secure forms of incident information handling to ensure protection of sensitive information at all times.