ASIFMA Principles on Harmonising Cybersecurity Incident Reporting

December 2024

Introduction

Cyber incident notification and reporting supports detection and response by providing early warning to the industry and insight into the cyber threat environment. When a malicious cyber incident causes significant harm to a firm, firms with a global footprint may need to report to dozens of jurisdictions with varying reporting requirements. The fragmented approach by authorities on cyber incident notification and reporting is increasingly burdensome, drives operational risk, and drains cyber resources. As firms dedicate their time and resources to meet compliance requirements rather than to mitigate incidents, it can be difficult to effectively manage operational and cybersecurity risk, and recovery.

Therefore, as governments and regulators consider legislative and regulatory cyber incident reporting requirements, the industry recommends that they harmonise their approaches to cyber incident notification and reporting.

1. Limit notification to incidents of significant actual harm driven by malicious intent

Incidents that rise to the level of notification should be narrowed to incidents that are driven by malicious intent and result in actual material impact or significant harm (i.e., severe disruption to critical operations, systemic risk, financial instability, major consumer harm, and/or public health and safety concerns). This would help avoid over-reporting of non-material cyber incidents that could divert an organisation's limited resources from incident response and remediation to incident reporting. Additionally, over-reporting of non-material cyber incidents would create unnecessary noise that diverts government resources away from proactive mitigation efforts on significant cyber incidents.

Incident response measures for malicious cybersecurity incidents have a different sense of urgency and action than a technology disruption with non-malicious intent. Behind a cybersecurity incident is an intelligent threat actor with specific motives. Therefore, those incidents are treated differently from the beginning, as the identity and elimination of the actor is sought, to the point of reconnection, where an evaluation of whether it is safe to continue business as usual is performed.

The highest value of a notification is that organisations can quickly communicate an early warning to authorities of an impending threat to their systems - even if all the details of an incident are not yet precise. Early warnings enable authorities to move swiftly to assist the institution or spread the word to other potentially impacted institutions.

2. Timing: when the ‘reporting clock’ starts running

Many jurisdictions have requirements that place a time limit by which incidents need to be reported to the regulators and other authorities and use the terminology of ‘becoming aware’ of an incident or something to this effect. This is meant to notify the authorities as soon as possible and avoid late notifications. The authorities can then use this information to communicate to the industry (as needed) in the event the incident may be a broader attack against that country’s financial sector, and for other firms to be alert of the current threats.

ASIA SECURITIES INDUSTRY & FINANCIAL MARKETS ASSOCIATION | Unit 3603, Tower 2 Lippo Centre | 89 Queensway Admiralty, Hong Kong | Tel: +852 2531 6500 www.asifma.org

'Becoming aware' should not be considered as the time when early notifications or alerts are raised by the organisation's surveillance and monitoring systems, as many of these alerts result in false positives. 'Becoming aware' should consider that a period of triage and analysis is required before an alert becomes something that could in fact be related to a cybersecurity incident. Once the firm determines to a reasonable degree of certainty that a cybersecurity incident is in progress or has occurred and that such incident has significantly harmed the confidentiality, integrity or availability of the organisation's computer systems compromising their ability to operate effectively, the reporting clock should then start, according to local regulatory requirements.

3. <u>Focus on a phased two-step reporting process</u>

The effective and efficient use of scarce resources to address a cyber incident must take precedence over regulatory reporting and real time data collection, especially in the initial phases of an incident. A phased reporting requirement is helpful in balancing the authority's need for timely reporting with the affected institution's primary objective of incident response.

I. **Step 1: Incident notification:**

A high-level, early warning to authorities of incidents of actual material impact (i.e., severe disruption to critical operations, systemic risk, financial instability, major consumer harm, and/or public health and safety concerns), despite institutions having limited information.

The clock that tracks the time limit for reporting to the regulators and other authorities starts running from the time the organisation confirms that an incident has reached their internal materiality threshold (as referred to in section 2 above). Upon indication of an issue and prior to submitting an initial report, an institution is assessing impact, therefore limited information may be available to report.

We recommend for the initial incident notification to take place when an institution confirms that an incident has reached their internal materiality threshold. This allows provision of a high-level, heads-up notification to regulators within a reasonable amount of time, similar to the 36-hour timeframe stipulated by the Interagency 'Computer-Security Incident Notification Requirements for Banking Organisations and Their Bank Service Providers'[1], in which the Inter-agencies specify "*… a banking organisation's primary Federal regulator must receive this notification as soon as possible and no later than 36 hours after the banking organisation determines that a notification incident has occurred.*" Given that there is limited information available to report, initial notification could focus on 1) data and time of identification of the incident and 2) initial observations.

The industry also suggests, in order to encourage and incentivise a culture of incident notification reporting, it is recommended that policies remove the fear of liability, financial sanctions, and regulatory enforcement actions.

After initial notification, an institution can provide updates to authorities when new information of significance to the incident is available. Authorities could share information, for example indicators of compromise, with the wider industry to mitigate any systemic impacts of the

[1] *Interagency (Office of the Comptroller of the Currency (OCC), Federal Reserve Bank (FRB), and Federal Deposit Insurance Corporation (FDIC)) 'Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers', 23 Nov 2021* https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank

incident. When sharing information, the authority should protect the identity of the firm reporting the incident.

II. **Step 2: Incident reporting (proportional to incident severity):**

After a firm assesses (e.g., by conducting a root cause analysis) and meaningfully mitigates an incident and the consequences thereof, a comprehensive analysis of the incident and its impact (with the level of details in proportion to incident severity), should be submitted to authorities. Following an incident, it may take anywhere from several weeks to months to determine the root cause, depending on the sophistication of the attack.

4. Harmonisation of data requirements

Data requirements for both incident notification and incident reporting have a high degree of commonality across jurisdictions, which presents an opportunity for further convergence and standardisation. Authorities should also take steps to harmonise reporting templates across jurisdictions such that reported information is consistent and easy to analyse. Useful resources include the U.S. Chamber of Commerce's 'Global Cybersecurity Incident Reporting' principles[2], the Financial Stability Board's (FSB) Format for Incident Reporting Exchange (FIRE) framework[3] (expected publication in October 2025), or similar efforts to harmonise incident reporting data fields and templates. Harmonised data fields and templates are useful to authorities in helping to conduct horizontal analysis of the most sophisticated attacks and to mitigate the potential for systemic impacts.

Conclusion

In conclusion, the proposed two-step reporting process offers a pragmatic solution that balances the need for timely notifications with the necessity of comprehensive post-incident analysis. By adopting a standardised approach, organisations can focus on the critical task of incident management, ensuring that resources are directed towards mitigation and recovery rather than compliance requirements.

The harmonisation of reporting requirements would also facilitate a more coordinated response to cyber threats, allowing authorities to analyse data more effectively and develop strategies that enhance the overall cybersecurity posture of the industry. The recommendations put forth in the principles, including the adoption of standardised reporting templates, underscore the importance of collaboration between regulatory bodies and the industry to achieve these goals.

---

[2] *U.S. Chamber of Commerce, 'Global Cybersecurity Incident Reporting', 14 Dec 2022, Vincent Voci and Danielle Muñoz*
https://www.uschamber.com/assets/documents/FINAL-Issue-Brief-Global-Cyber-Incident-Reporting.pdf

[3] *Financial Stability Board, 'Format for Incident Reporting Exchange (FIRE)', 13 Apr 2023*
https://www.fsb.org/uploads/P130423-2.pdf