ITI Promoting Innovation Worldwide

ITI Global Policy Principles for Security Incident Reporting

September 2021

As the cyber threat landscape continues to evolve, and cybersecurity compromises become more frequent, policymakers around the world have increasingly turned to incident reporting regimes as a potentially appropriate tool to gain greater visibility into such compromises. The proposals introduced to date often conflate multiple issues and misunderstand the goals and the applicability of security incident reporting.

ITI recognizes the importance of cybersecurity incident reporting to inform actions to respond to incidents and to contain or prevent further impacts. ITI views the concept of an incident in this context as distinct from a vulnerability, cyberthreats, or a data breach (see box for details). If an incident report provides sufficient technical details about the suffered incident, competent authorities within the government can understand the nature of the attack and take steps to mitigate the associated risk. Likewise, actionable incident reporting may help competent authorities to prioritize incident response assistance to affected organizations who require support, particularly while dealing with an active campaign targeting multiple organizations. Finally, in the aggregate, robust incident reporting may provide governments with a more complete picture of the threat landscape.

As such, if carefully crafted, incident reporting has the potential to be a helpful policy lever, assuming the principles articulated below have been fully adopted. It is through this lens that we offer our

Security incident reporting is distinct from other concepts with which it is often confused: data breach notification, cyberthreat information sharing, and coordinated vulnerability handing and disclosure. While some incidents may blur the line between these concepts or implicate more than one, it is important to understand the difference between these terms and what each measure is meant to achieve.

Security Incident Reporting *generally focuses on the past because it reports on the details of a cybersecurity incident that has already occurred. This could include the vector of compromise, the systems and information compromised or targeted by the attacker, and any attributes of the attacker's behavior. Reports may focus on the actual or potential harm caused by an incident. Information conveyed in the reporting highly depends on the reporting timeline, reporting purpose (and use) and segment needs.*

Data Breach Notification *relates specifically to the unauthorized access to or disclosure of personally identifiable information or other sensitive privacy data. In the United States, there are more than 50 state and local laws focused on data breach notification.*

Cyberthreat Information Sharing *is forward-looking and refers to the proactive sharing of cyber threat information to help all entities understand threats and take steps to prevent successful cyberattacks. Threat information sharing should be voluntary and may include indicators such as anomalous network activity or methods of circumventing security controls.*

Coordinated Vulnerability Handling and Disclosure *(CVD) focuses on the processes associated with vulnerabilities, which are distinct from incidents. If exploited, in certain cases, vulnerabilities may constitute an incident (as defined), but generally that is not the case – the goal of vulnerability handling processes is to limit potential harm to end users by developing mitigations and releasing them to prevent exploitation. CVD processes, international standards (ISO/IEC 29147 and 30111), and best practices appropriately limit and protect information disclosed to entities essential to the CVD process, prior to public disclosure.*

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

recommendations on the key areas that global policymakers must consider in developing an effective, efficient security incident reporting regime.

Develop and Adopt an Incident Categorization Model

Policymakers should ensure that the threshold for reporting requirements is mapped to specific criteria and specific incident severity levels related to identifiable harms, such as to public health and safety, or operational disruption.[1] Reporting requirements should only focus on severe and significant attacks that cause actual disruption or loss and should include specific parameters. An incident categorization model or matrix[2] can represent the severity of an incident more accurately which helps with the prioritization of incidents and ultimately supports more precise reporting. Focused reporting that is limited to severe incidents reduces the burden on information security teams and frees up resources for the essential tasks of examining and remediating incidents and securing the organization's systems. Moreover, it reduces the likelihood of an informational overload for applicable authorities that would undermine their ability to prioritize responses and divert limited agency resources from critical risk mitigation activities. These considerations are also key in the context of defining the scope and object of reporting (e.g., avoiding the confusion of 'incident' with other concepts or expanding to 'potential' incident reporting). We recommend policymakers advance the joint understanding of the matrix and severity concept, by facilitating consensus-driven processes.

Establish Feasible Reporting Timelines Commensurate with Incident Severity Level

Any incident reporting policy proposal should ensure that reporting timelines are aligned with global best practices. The required timelines should be commensurate with incident severity levels but allow for at least a 72-hour reporting window after an entity has verified the incident. Anything shorter is unnecessarily brief and injects additional complexity at a time when entities are more appropriately focused on the difficult and resource-intensive task of understanding, responding to, and remediating a cyber incident. Shorter timelines also greatly increase the likelihood that the entity will report inaccurate or inadequately contextualized information that will not be helpful, potentially even undermining cybersecurity response and remediation efforts. Furthermore, since the information available 72 hours after the incident may be limited, we advise policies to allow for a flexible approach, where more complete information can be provided after a longer period of time and updated as additional information is acquired. This period of time should be no shorter than a month.

Limit Incident Reports to Confirmed or Verified Incidents

Incident reporting requirements should be limited to confirmed or verified incidents, as opposed to requiring entities to require "potential incidents" or "near misses." Requiring the reporting of "potential" incidents does little to improve cybersecurity and could inadvertently create an information overload, preventing the competent authority from prioritizing actual, confirmed incidents, and undertaking appropriate action to respond, particularly when it is not clear what would constitute a "potential" incident. It may also divert resources away from information security teams within organizations, who should be focused on responding to significant incidents, instead of expending those resources to report potential incidents or near misses. Reporting verified or confirmed incidents

[1] Currently, the US approach to categorizing cyber incidents in the National Cyber Incident Response Plan defines a "Significant Cyber Incident" as a cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

[2] Similar approaches have been proposed by CISA and are already adopted by the UK and Australia.

that have been well-defined and scoped will help to avoid a culture of overreporting that will strain limited incident response capacity and capabilities inside and outside the government. It will also help ensure that information received is useful and actionable.

Limit Responsibility for Reporting Only to the Compromised Entity

Any incident reporting policy proposal should ensure that the reporting obligation falls only on compromised entities. Vendors and third-party service providers should not be required to report to competent authorities cybersecurity incidents that have occurred on their customers' networks. Such a requirement would pose numerous challenges to normal business operations, including potentially forcing vendors or third parties to disclose business confidential information of such customers or breach their contractual obligations. Additionally, many vendors and service providers operate globally, so broad reporting requirements would not only affect business operations but would potentially cause international conflicts of law. Finally, since incident responders often operate on retainer or are called in only in the event of a breach, they would be unlikely to have additional useful information to report, and any information provided would be duplicative of what the compromised entity is already required to provide. Therefore, a requirement that captures third-party providers to also report an incident risks diverting resources at critical initial moments and, in the long term, could risk discouraging companies from engaging third-party services entirely.

Ensure Confidentiality and Appropriate Protections around Sensitive Information Shared with or by Competent Authorities within the Government, including Against Regulatory Use

It is imperative to have strong and transparent rules about the confidentiality and use of incident information that is shared with or by competent authorities within the government. Such rules should govern not only the protected dissemination of incident information with regulatory authorities but should preclude direct or indirect regulatory use of such information. Such rules should additionally govern how unclassified information on a specific incident is further shared within the government, with other governments, and with nongovernmental entities. These rules must be crafted to guarantee compliance with existing legal regimes, including contractual, IP, and privacy obligations and the protection of end users. A designated centralized reporting agency should provide a secure method of communication. This could be as simple as publishing a PGP encryption key or using the Traffic Light Protocol (TLP). Trust is essential. More generally, information dissemination should be done in a manner consistent with international standards and industry best practices.

Establish or Maintain Appropriate Liability Protections and Ensure Information Provided is Exempt from Public Disclosure

Entities providing incident reports should receive liability protections for providing such information to competent authorities. Indeed, it is important that any policy maintains appropriate liability protections, so that information provided in a report cannot be used at a later date against the reporting entity, except in instances where entities have engaged in willful or illegal misconduct. Information about a security incident received by competent authorities should also be exempt from public disclosure under appropriate national laws.

Ensure that Cybersecurity Incident Reporting Requirements are Aligned

In developing any new, comprehensive incident reporting proposal, policymakers should ensure that requirements are aligned to avoid duplication. Policymakers should undertake an analysis of the current cyber incident reporting landscape in their jurisdictions, including sector-specific notification or

national-level requirements. In doing so, policymakers should also make note of data breach notification requirements, which often stem from the same incident. If needed, officials should consider how to consolidate or otherwise streamline existing regulatory reporting requirements.

Designate a Single Point of Contact for Companies to Report Security Incidents to within the Government

Incident response and recovery resources are in short supply. To effectuate the efficient use of limited resources, governments should designate, and adequately fund, a single point of contact for all organizations that need to report an incident. In the event that existing reporting requirements have not been harmonized and sector-specific reporting requirements remain in place, impacted organizations should not be required to report an incident twice.

Define an Appropriate and Flexible Reporting Template

Incident reports should follow a standardized template to ensure consistent reporting. Consensus-driven processes are needed to refine the elements of such a template to ensure consistency with existing frameworks, like MITRE ATT&CK or VERIS, and international industry best practices, as well as to ensure that the template fits the needs and existing practices of a particular sector. Reporting entities can use such a template to report the most relevant information where available. By way of example, the template may include appropriate and reasonably obtained information on 1) the attack vector or vectors that led to the compromise; 2) the indicators of compromise and related information on the affected systems, devices, or networks; 3) information relevant to the identification of the threat actor or actors involved; 4) a point of contact from the affected entity; and 5) impact, earliest known time, and duration of compromise.[3] Entities should have the option to report additional types of information on cybersecurity incidents to help to identify emerging trends or otherwise preempt attacks. Entities should also not be penalized for or precluded from reporting an incident if all information, including the information proposed in this list, is not available.

Align Reporting Processes and Mechanisms to Ensure Consistency with Industry Best Practices and Allow for Bi-Directional Information Sharing

The protocols and mechanisms of reporting an incident should be consistent with existing frameworks as well as recognized sectoral, international, and industry best practices. To ensure incident information is shared quickly and continuously, governments should ensure that there are processes or mechanisms in place that streamline and allow for bi-directional sharing of incident information.

Build Competent Authority Capability to Take Action on Security Incident Reports

Security incident reporting will be of limited utility if the designated competent authority does not have the capacity to ingest and take action on the information it receives. A manual-intensive approach will quickly max out resources and elevate the risk that important alerts are inadvertently missed. Before a security incident reporting scheme is established, the designated competent authority should have the capability to automate data collection so that internal data can be cross-referenced with externally available data. This will inform and improve the orchestration of incident response actions.

---

[3] This initial list is based on the following CISA documents: https://www.cisa.gov/sites/default/files/publications/Law%20Enforcement%20Cyber%20Incident%20Reporting.pdf https://www.cisa.gov/sites/default/files/publications/Non-Federal%20Entity%20Sharing%20Guidance%20under%20the%20Cybersecurity%20Information%20Sharing%20Act%20of%202015_1.pdf; other resources are available: https://us-cert.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf.