ITI Promoting Innovation Worldwide

ITI Policy Principles for Security Incident Reporting in the U.S.

July 2021

The SolarWinds compromise has demonstrated how the cyber threat landscape is constantly evolving, resulting in the emergence of new threats. In search of a suitable policy response, policymakers have increasingly turned to incident reporting policy regimes as a potentially appropriate tool. 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 concepts related to security incident reporting as distinct from those of cyber threat information sharing or a data breach notification (see box for details). If a report provides sufficient technical details about the suffered incident, federal agencies can understand the nature of the attack and take steps to mitigate the associated risk. Likewise, actionable reporting may help government officials to prioritize incident response assistance to affected organizations, particularly while dealing with an active campaign targeting multiple organizations. This assumes that affected organizations required support and that the principles articulated below have been fully adopted.

As such, if carefully crafted, incident reporting has the potential to be a helpful policy lever. It is through this lens that we offer our recommendations on several key areas that policymakers should consider in developing an effective, efficient security incident reporting regime.

Security incident reporting is distinct from other concepts with which it is often confused: data breach notification and cyberthreat information sharing. While some incidents may blur the line between these concepts, it is important to understand the difference between these terms and what each process is meant to achieve.

Security Incident Reporting *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 the 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 *focuses on the future and refers to the proactive sharing of 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.*

Develop and Adopt an Incident Categorization Matrix

Policymakers should ensure that the threshold for reporting requirements is mapped to specific objective criteria and specific incident severity levels related to identifiable harms, such as to public

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

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 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 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 policy makers advance the joint understanding of the matrix and severity concept, by facilitating a consensus-driven processes.

Establish Feasible Reporting Timelines Commensurate with Incident Severity Level

Any incident reporting legislation should ensure that 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 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.

Limit Responsibility for Reporting Only to the Compromised Entity

Any legislation should ensure that the reporting obligation falls only on compromised entities. Vendors and third-party service providers should not be required to report cybersecurity incidents to the US Government 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 that customer or breach their contractual obligations.

Ensure Confidentiality and Appropriate Protections around Sensitive Information Shared with Federal Agencies, including Against Regulatory Use

It is imperative to have strong and transparent rules about the confidentiality of incident information that is shared with or by federal agencies. Such rules should govern not only the dissemination of incident information with relevant interagency partners but should specifically preclude direct or indirect regulatory use of such information. Such rules should additionally govern how unclassified information on a specific incident is further shared with the US Government, other governments, and with nongovernmental entities. These rules must be crafted to guarantee compliance with existing legal regimes, including contractual and privacy obligations. 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.

---

[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.

Establish Targeted Liability Protections and Appropriate Exemptions from the Freedom of Information Act (FOIA)

Entities providing incident reports should receive liability protections for providing such information to federal agencies, including engaging in activities related to monitoring or network awareness of their information systems, other than in instances where entities engage in willful misconduct. Additionally, cybersecurity incident reports shared with the US Government should be exempt from FOIA requests.

Harmonize Federal Cybersecurity Incident Reporting Requirements

There are currently several different measures that govern federal cybersecurity incident reporting, making for a complex and oftentimes confusing landscape.[3] To alleviate such confusion, Congress should consider harmonizing existing regulatory reporting requirements to ensure the efficient sharing of covered cybersecurity incidents.

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, the federal government should designate, and adequately fund, a single point of contact for all companies that need to report an incident. If 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. All future legislative proposals should designate CISA as the single point of contact where no sector-specific regulator exists, and appropriate resources should be allocated for that purpose.

Define an Appropriate and Flexible Reporting Template

All incident reports should follow a standardized template to ensure consistent reporting across agencies and industries. 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; 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.[4] 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.

---

[3] See, for example, banking sector notification requirements: *12 CFR part 30, appendix B, supp. A (OCC); 12 CFR part 208, appendix D-2, supp. A, 12 CFR 211.5(l), 12 CFR part 225, appendix F, supp. A (Board); 12 CFR part 364, appendix B, supp. A (FDIC) (italics omitted); NPRM on Computer Security Incident Reporting Requirements for Banking Organizations and their Bank Service Providers;* defense industrial base mandatory reporting requirements: *32 CFR § 236.4 - Mandatory cyber incident reporting procedures;* FISMA reporting requirements: 44 U.S.C. §§ 3553-54 & associated Binding Operational Directive 16-03; FedRAMP Incident Communications Procedures; NERC *Incident Reporting and Response Planning* as required by FERC; and US-CERT Federal Incident Notification Guidelines.

[4] 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.

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, recognized sectoral, international, and industry best practices. To ensure incident information is shared quickly and continuously, sections 2.f and 2.g of Executive Order 14028 direct improvements to the inter-agency sharing of incident information. In addition to these provisions, federal agencies also need to streamline legal agreements involving industry partners to allow for bi-directional sharing of incident information.

Build Agency Capability to Act on Security Incident Reports

Security incident reporting will be of limited utility if the designated recipient agency does not have the capacity to ingest and act 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 recipient agency 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.