U.S. Chamber of Commerce

1615 H Street, NW
Washington, DC 20062-2000
uschamber.com

Global Cybersecurity Incident Communications: Notification, Reporting, and Information Sharing Policy Brief

The world is increasingly interconnected through digitalization, and cybersecurity threats are becoming more sophisticated, well-funded, and persistent. The most significant cybersecurity incidents can impact economic stability, public health and safety, or national security interests. Both public and private sectors must work together to reduce the risk of significant incidents. Industry is working diligently to mitigate cybersecurity risk and to take concrete steps to protect information systems and data stored on those systems. Cyber incident notification and reporting are tools to support detection and response by early warning to industry and providing insight into the cyber threat environment. However, the fragmented approach by authorities[1] on cyber incident notification and reporting is increasingly burdensome and drains cyber defense resources without adding value to cybersecurity risk management.

This policy brief is intended for global authorities to inform future cyber incident notification and reporting policies and harmonize and standardize reporting and processes. We are committed to working with authorities on sound cybersecurity incident notification and reporting principles and practices that will best serve the public and private sectors. The principles laid out in this brief are a critical step towards a safer cyberspace that enables innovation, job creation, and breaks down barriers to businesses operating globally.

Recent legislation, regulation, and policies worldwide have focused on mandatory cybersecurity incident notification, reporting, and public disclosure. As governments consider legislative and regulatory cyber incident reporting requirements for industry, they should consider impacts on global cybersecurity operations while standardizing and harmonizing key provisions. The recommendations in this policy brief are neither comprehensive nor exhaustive; instead, they represent a critical element of effective cyber incident reporting regimes.

1. **Identifying discrete policy objectives and related requirements:** Cybersecurity incident reporting and incident management requirements should align with policy objectives to ensure that authorities receive information at the right time, with the right level of detail, and without causing unnecessary drain of resources during critical moments in incident response. Clarifying objectives will also enable authorities to assist the private sector in incident management and, therefore, better incentivize the private sector to notify authorities of confirmed, significant cyber incidents.

   The Chamber urges authorities collecting reported data to clearly articulate why covered critical infrastructure must report incident information, how authorities will use it to reduce cyber risk, and what authorities will bring resources for incident response.

[1] Authorities in this document may refer to a variety of government agencies with several important roles in cybersecurity for critical infrastructure, including but not limited to the following types of agencies: computer emergency (or incident) response teams, competent authorities, government agencies, sector risk management agencies, regulators, or lawmakers.

There are four primary policy objectives related to cybersecurity incidents:

- Early warning to authorities of a significant cybersecurity incident that could impact the broader ecosystem or an incident with contagion risk. In pursuit of this objective, policymakers should apply liability, financial, and regulatory incentives to institutions that sound the alarm quickly despite having limited information. For early warning, authorities should write policies that allow an institution to fully deploy resources towards mitigating the incident and not overly focus on reporting.

- Enable authorities to identify trends, common threats, or analysis of the efficacy of security controls. In pursuit of this policy objective, authorities collect incident data from multiple incidents across critical infrastructure to enable them to better understand the threat landscape in the aggregate. Widely recognized private sector examples of threat reports include the Verizon Data Breach Investigations Report or Cybercrime Magazine's market research reports. Authorities should also take steps to harmonize reporting templates across jurisdictions such that reported information is consistent and easy to analyze.

- Uplift of industry's resilience and prevention of cyber threats. Information-sharing forums should be leveraged or established to enable real-time information sharing of potential threats and known vulnerabilities. This type of sharing should always be voluntary and confidential. Mandatory information-sharing with authorities tends to have the opposite effect in driving institutions to share less, especially if there are inadequate liability protections.

- Cybersecurity incident impact assessment and response. Notification and reporting requirements under this policy objective are primarily for after-action analysis to better understand the root cause, impact, and evaluate the effectiveness of public and private sector responses.

2. **Distinguish Differences Among Notification, Reporting, and Information Sharing:** For purposes of this document, we refer to three types of communication related to incidents:

    - *Incident Notification.* A high-level, early warning to authorities of incidents of significant impact (i.e., threatens economic stability, public health and safety, or national security), despite institutions having limited information. Policies should incentivize a culture of incident notification and remove the fear of liability, financial sanctions, and regulatory enforcement action.

    - *Incident Reporting.* After a firm assesses and meaningfully mitigates an incident, a more detailed analysis of the incident and its impact is submitted to authorities.

    - *Information Sharing.* Voluntary, ad hoc sharing of information amongst peers that includes analysts' observations of vulnerabilities, suspicious activities, or indicators and warnings.
        - Examples of information-sharing forums include Information Sharing and Analysis Centers (ISACs), Computer Emergency Response Teams (CERTs), and Computer Security Incident Response Teams (CSIRTs).

- In the U.S., the Analysis and Resilience Center (ARC) comprises U.S. government intelligence analysts and analysts from the financial and energy sectors to monitor malicious activities against critical infrastructure.

The table below outlines the data requirements for the notification and reporting policy objectives:

Policy Objective	Definition	Requirements
Notification	An initial high-level alert to authorities within 72 hours after establishing that an incident is significant.	▪ Name of victim ▪ The date incident was confirmed ▪ Type of incident (e.g., ransomware, business email compromise, financial loss, denial of service, destructive attack, reputational attack, or loss of data confidentiality or integrity) ▪ Impacted systems and their functions ▪ Potential vulnerabilities exploited ▪ Is there a ransom demand? If so, is there a virtual wallet or mechanism for ransom to be paid?
Reporting	A more detailed analysis of the incident and its impact is submitted to authorities after a firm assesses (e.g., root cause analysis) and meaningfully mitigates an incident (e.g., within 30 days).	▪ Root cause analysis ▪ MITRE ATT&CK categories or vector of compromise ▪ Tactics, techniques, and procedures (if known) ▪ Technical information (e.g., IP addresses, hashes, indicators of compromise, signatures) ▪ Malware employed ▪ Zero-day exploit used (if known) ▪ Level of impact ▪ Information impacted, which may include the type of information lost, compromised, or corrupted. ▪ Scope of time and resources needed to recover from the incident ▪ Threat actor information (if known) or communication

3. **Provide robust liability protections for notification and reporting of incidents to authorities.** Policies should establish that the notification and reporting of a covered incident and the contents of any notification or report, including supplemental reporting, are confidential and protected from legal liability. Information contained in notifications and reports should not be subject to discovery in any civil or criminal action. Reporting entities, in essence, should not be penalized after the fact for complying with a legal or regulatory obligation.

   Further, policies should ensure compliance with incident notification and reporting requirements is supportive, not punitive. Policies must create a compliance regime that treats companies subject to cyberattacks as victims. A reporting regime must encourage cooperation and strengthen trust between the public and private sectors. A regulatory-based approach that focuses on punitive actions, such as fines or penalties, rather than mutual gains would counter the goal of creating a robust partnership model to address the increasing cyber threats facing the public and private sectors globally.

4. **Establish an incident notification timeline of no less than 72 hours.**[2] Incident notification timelines are a priority for governments around the world. These policies should reflect risk-based, flexible standards for notifying authorities about significant cyber incidents. Effective reporting timelines must align with policy objectives and international norms while balancing notification and reporting with external stakeholder cooperation (e.g., law enforcement), response, and remediation.

   Timelines should strive to avoid injecting additional complexity at a time when affected entities are focused on the difficult task of understanding, responding to, and remediating a potential cyber incident. Affected entities need time to investigate an intrusion before reporting it to an authority. They should provide notification of an incident once it has been able to conduct initial mitigation and response efforts or thwart mitigation efforts. However, the details of a notification should be for authorities only and not be publicly disclosed so as not to disrupt or expose sensitive investigative efforts. Even relatively minor cyber incidents can absorb enormous resources to assess an incident's scope and impact accurately.

   Proposed rules that compel companies to make premature public disclosures driven by compliance timelines rather than remediation controls may place companies and the public at greater risk. Hasty reporting requirements could generate inaccurate or incomprehensive reporting. For example, incident severity could be overstated, leading to temporary, time-limited negative consequences in the market or investor confidence. It also can risk inaccurate reporting before an incident is fully understood and mitigated.

   The Chamber encourages global harmonization of incident notification timelines no less than 72 hours after an affected entity confirms a significant cyber incident. Doing so will ensure that reporting entities can provide information to the government or the public that is comprehensive, properly contextualized, and as accurate as possible at the time of reporting.

[2] For systemic events, institutions should attempt to notify authorities earlier than 72 hours for the greater good of the system.

5. **Notify and report only on confirmed cyber incidents.** Industry needs clarity on notification requirements, which should only be triggered by well-defined, confirmed, and harmful cyber incidents. Policies that require incident notification for potential cyber intrusions and incidents that could be reasonably believed are overly subjective. This subjectivity could lead to over-reporting—burdening the affected entity and authorities. Confirmed cyber incidents that trigger notification to authorities should be clearly and objectively defined to promote an appropriate reporting balance.

6. **Limit notification to incidents of significant harm.** The highest value of notification is that institutions can quickly communicate an early warning to authorities of an impending problem in the system—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. As such, incidents that rise to the level of notification should be narrowed to avoid over-reporting and creating unnecessary noise that could divert an organization's limited resources from incident response and remediation to incident reporting, and divert government resources from proactive mitigation efforts on significant cyber incidents.

7. **Limit reporting to incidents of actual harm by a malicious actor driven by malicious intent.** The Chamber has observed policies that require businesses to report activities, such as probing or scanning, which are everyday occurrences. Overly broad notification and reporting requirements such as these cause significant resource challenges for businesses, creating a vast number of cyber events of comparatively little importance. Authorities should also consider that reporting cyber events or temporary time-limited operational outages of insignificant or no impact creates ineffectual analysis and inefficient deployment of resources. Covered critical infrastructure seeks analysis of significant cyber incidents where harm and impact have been assessed, and it can deploy appropriate response activities.

   The Chamber supports policies that align notification and reporting requirements to significant cybersecurity incidents resulting from a malicious actor with malicious intent. For institutions, the criticality of notification and reporting has a different sense of urgency and action for incidents resulting from an intelligence threat actor with specific motives than an incident resulting from a non-malicious technology disruption.

   The Chamber believes that definitions for reportable cyber incidents need refinement and boundaries. Policymakers should not interpret definitions overly broadly or subjectively. Definitions of reportable cyber incidents should track more closely with the following:

   - U.S.: Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
   - APAC: Australia's Security of Critical Infrastructure Act 2018.
   - EMEA: Network and Information Security (NIS) 1 Directive.[3] Cross Market Operational Resilience Group (CMORG) Incident Lexicon.

[3] Note: at the time of this writing (December 7) the European Council has adopted the NIS 2.0 Directive, but it has not been published in the European Journal. Upon publication the EMEA bullet will be updated to reflect it's entry into force.

8. **Harmonize notification and reporting requirements.** Several critical infrastructure sectors have existing obligations to report significant cyber incidents to authorities. In the case of firms with operations in dozens of countries, it is routine to have national reporting, sector, and regulator requirements. The Chamber implores policymakers to recognize that conflicting and duplicative reporting requirements are burdensome and distracting from the underlying policy interest. Future efforts must focus on aligning global notification and reporting requirements to ensure that industry resources are used efficiently to combat cyber threats rather than customizing reports on the same incident for multiple authorities. Authorities should agree on a common set of information to be reported that can be used for numerous agencies and across geographic boundaries.

   The Chamber has urged public and private stakeholders to work towards harmonizing duplicative and overly burdensome cybersecurity notification and reporting requirements that impact regulated institutions. Notification and reporting requirements should articulate a policy objective and a reasonable plan to harmonize the myriad cyber regulations and laws that impact industry. Efforts through existing forums like the Group of Seven (G7) or the Quad may be leveraged to identify and make progress toward notification and reporting harmonization. Authorities can look to the U.S. Cyber Incident Reporting Council, the Financial Stability Board (FSB), or similar efforts to harmonize incident reporting requirements.

9. **Ensure government use of reported data is adequately protected**. Reporting policies and procedures should consider the security controls authorities have to protect data collected from notification and reporting.

   Government use of data should:

   - Exempt reported information from any existing disclosure laws and regulatory use;
   - Treat shared information as commercial, financial, and proprietary;
   - Waive governmental rules related to *ex parte* communications; and
   - Preserve trade secret protections and any related privileges or protections.

   Reporting policies and procedures need to put a premium on protecting open vulnerability information and incident data from premature public disclosure. One exception should be an allowance for law enforcement to have access to reported data for criminal investigations of cybercriminals. Such access should be balanced with protections for the reporting victim. Governments must ensure that procedures for sharing incident data are consistent with international standards and industry-developed best practices for protected and confidential data exchange.

10. **Manage public disclosure of cybersecurity incidents, especially unmitigated incidents.** Cybersecurity incident notification and reporting to authorities and law enforcement is beneficial because it can improve the overall system's security. Authorities and law enforcement agencies serve as a central collection point where incident notification and reporting data (e.g., early warning, remediation strategies) can be analyzed, anonymized, and distributed to other institutions to help them better defend their networks. However, authorities must manage the use of incident notification and reporting data to ensure public disclosure of incident data does not occur prematurely—or at all in the case of unmitigated incidents. Reporting and notification policies must balance security and disclosure, especially for unmitigated incidents. In many cases, public disclosure may increase the risk of re-victimization or further exploitation of impacted firms.

11. **Include temporary delays for ongoing investigations.** Organizations who are victims of cyber incidents must be afforded temporary reporting delays when they are part of ongoing law enforcement or national security investigations against illicit hackers. Policies should facilitate cooperation by victims with law enforcement and national security agencies to mitigate the impacts of cyber incidents without re-victimizing the victim. Some jurisdictions have passed laws authorizing delayed disclosures to consumers when personal data breaches occur to avoid compromising ongoing law enforcement investigations.[4]

12. **Limit reporting to a victim entity or its designee.** A critical consideration in cyber incident reporting policies is who should be allowed to file a notification or report and preserve the contractual relationships between industry partners in the ecosystem:

    - Cyber incident notification and reporting policies should limit the ability to notify or report to the victim entity or its designee.

    - Critical infrastructure owners and operators should be allowed to manage incident reporting from their suppliers through contracts. This approach would ensure governments are made aware of cyber incidents without jeopardizing trusted relationships between industry partners. It would also help avoid duplicative reporting regarding the same incident. For example, in the case of cloud services, there is a shared responsibility for securing physical infrastructure and the virtualized platform. There should be clarity about that the obligation to report is with the impacted critical infrastructure entity to avoid duplicative or inconsistent reporting by cloud service providers and their critical infrastructure clients CSPs and their customers also should be permitted to clarify any incident notification or reporting responsibilities through contractual obligations.

    This approach would avoid unintended outcomes like compelling cybersecurity providers to disclose the sensitive business information of their clients, breach contractual obligations, and dissuade businesses from employing outside experts to the detriment of a critical infrastructure entity's cyber defenses.

[4] R Street Institute. "Cybersecurity Incident and Breach Reporting Requirements." June 23, 2022. https://www.rstreet.org/2022/06/23/cybersecurity-incident-and-breach-reporting-requirements/

13. **Treat reporting as a means to bidirectional sharing and collaboration.** Cybersecurity information sharing must be bidirectional between the public and private sectors. Information reported to government needs to be promptly aggregated, anonymized, analyzed, and shared with industry to mitigate future cyber incidents. A persistent shortcoming experienced by businesses across many sectors is a need for timely and effective action or feedback on cyber reports from the government. Cyber incident notification and reporting policies must turn reported information into value-added risk management tactics, techniques, and procedures for network defense. Quality intelligence comes not from coerced reporting but from deliberate cooperation and trusted public and private relationships.

14. **Ensure any rulemaking or legislative processes include substantial industry input.** The Organization for Economic Cooperation and Development (OECD) highlights that stakeholder engagement is a crucial element of regulatory policy. It helps ensure that regulations are in the public interest by involving those affected by regulations, including citizens, businesses, civil society, and other community members. It also ensures that regulation is user-centric and responds to the needs of those governed, and that regulatory requirements are practically implementable. By consulting all affected bodies, stakeholder engagement enhances the inclusiveness of policies and supports the development of a sense of ownership. Stakeholder consultation strengthens trust in government, social cohesion, and compliance with regulations.

    When drafting new reporting requirements for the private sector, drafters should include a reasonable comment period for industry feedback and collaboration. Coordination with impacted industry entities is critical because they can provide valuable input on many programmatic details, such as definitions and reporting contents. Should the rulemaking process identify issues that warrant further industry expertise, an additional public consultation period may be required.

    Without stakeholder engagement by governments before releasing mandatory cyber incident reporting proposals, there may be a negative impact on cybersecurity for organizations, and at worst, result in redundant or inconsistent approaches across jurisdictions, regulatory bodies, and other agencies and undermine security.

15. **Government authorities should adopt a prioritized, risk-based scope of covered entities.**

    Government authorities should adopt a prioritized, risk-based approach to assess the scope of covered entities to which mandatory significant cybersecurity incident notification and reporting requirements apply. Authorities should not rely on open-ended definitions of critical infrastructure. Specifically, the definition of covered entities should be tightly construed to include only those entities whose operations and functions pose an immediate, high-level risk with severe and adverse consequences to national security, economic security, or public health and safety.

From a risk management perspective and for the purposes of notification and reporting requirements, the Chamber believes that the scope of covered entities should be a subset of critical infrastructure entities. For mandatory notification and reporting to be effective, authorities should establish criteria that creates a narrow list of covered entities within a critical infrastructure sector that, if impacted, would result in significant consequences. Otherwise, receipt of reports from an overly broad list of entities with different reporting standards could risk creating unintended noise in the system that detracts from the objective of protecting critical infrastructure.

It is in the public and private sector interest that authorities take an incremental approach to designating covered entities. A list of covered entities should be limited in reach and risk-based. Rather than focus on an elusive number of entities to cover, the Chamber urges authorities to focus on the types of significant cyber incidents that it wants covered critical infrastructure to report. In other words, consideration should be given to emphasizing a significant incident—rather than the entity.

The Chamber urges critical infrastructure and authorities to engage in a full spectrum of operational collaboration, information sharing, and cybersecurity risk management activities in steady state. A disciplined, risk-oriented approach would advance policymakers' goal of moving from traditional public-private partnerships to public-private operational collaboration.