# Incident Handling Procedures

This issue examines the challenges governments, cloud providers, and other stakeholders (for example, enterprise customers, insurers, and others) face in their handling of cloud incidents[1] —comprising (1) preparation, (2) detection and analysis, (3) containment and eradication, and (4) postincident evaluations and evidence retention.[2] There also exist challenges relating to incident recovery efforts, particularly those that pertain to preparedness and postincident activities, which are analyzed in the Resilience basket.

## Key Considerations

- ***Need to broaden the understanding of cloud "incidents."*** Stakeholders risk focusing on incidents arising from the exploitation of more traditional cybersecurity vulnerabilities to the exclusion of other nonmalicious triggers of digital failure, such as human errors and technical failures, supply chain disruptions, natural disasters, and more. Moreover, though unlikely,[3] there is a need to account for vulnerabilities that affect different cloud providers and their customers that, if exploited, can impair operations across one or more major cloud provider's services.
- ***Ambiguity in the allocation of responsibilities among stakeholders.*** As these topics are commonly addressed in contracts between cloud providers and their enterprise customers, there is no uniform template or widely accepted standard for division of responsibility between the various stakeholders involved in a cloud incident, including regarding notifying affected individuals and pertinent government authorities, addressing the threat, and more. For example, the targeting of cloud services by nation-state actors complicates incident response efforts, as governments have traditionally been responsible for countering nation-state actors while providers have generally only played supportive roles.
- ***Different incident reporting rules.*** Policies vary with respect to when, whom, how, and in what format an entity must report a known incident both across and within nations. Additionally, it is possible that this patchwork of requirements could cause delays in providing notice to affected individuals, organizations, and relevant government authorities (or prevent them from providing notice entirely). Navigating different jurisdictional requirements presents burdens that a single standard of practice might avoid, and it also may incentivize companies to find reasons to avoid reporting. Moreover, the close coupling of cloud providers and their enterprise customers creates significant shared responsibilities, which complicate efforts to inform relevant entities and respond to cloud incidents.
- ***Stakeholders lack information sharing tools and arrangements.*** Providers and government actors may lack the tools and arrangements[4] necessary to ensure their situational awareness and share real-time information with other stakeholders (including foreign entities) in order to assist with threat hunting and incident-response coordination. The lack

of a centralized authority[5] or mechanism to manage incident reporting and coordination for the cloud sector[6] may lead to a fragmented response by stakeholders, especially when such efforts require incident data collection from various third parties (such as internet service and other cloud providers) or data residing in multiple locations.[7] This challenge also extends to cloud providers sharing information with affected entities, who may wish to receive timely notice about any incidents affecting cloud services.

- ***Weak reporting incentives.*** Some stakeholders may hesitate to disclose incidents because of the financial and reputational costs associated with doing so, as well as the liability that might follow from it. As a consequence, it is possible that important information about incidents that could be part of a larger mosaic in understanding the incident at hand, and trends in cyber crime more broadly, remain unknown to government authorities.
- ***Concerns over privacy of commercially sensitive information.*** Providers and enterprise customers may feel reporting requirements to be imperfectly protective of commercially sensitive information, potentially dissuading them from reporting incidents.

## Stakeholder Perspectives

### Government

- Seek notices about cloud incidents from service providers and other affected entities to gain insight into the causes of failure and possible remedial action. (Similar to Cloud Providers', Customers', and Insurers' perspectives.)
- Some wish to establish a government-led incident reporting and threat-hunting process.
- Wish to decide whether and how to intervene in

### Providers

- Seek collaboration with other stakeholders in their efforts to safeguard against cloud incidents that may threaten to interrupt services. (Similar to Customers' perspective.)
- Welcome greater threat intelligence sharing between government and private sector actors, so long as they do not have to disclose more than they are comfortable with.
- Seek to inform government efforts to

### Customers

- Prioritize implementing tools and procedures that help prepare for cloud incidents and minimize their disruptive effects.
- Wish to have insight into incidents and responses from providers and governments.[10] (Similar to Governments', Cloud Providers', and Insurers' perspectives.)
- Seek compensation for damages incurred (including identity-theft protection, if appropriate or required).
- Seek an increased understanding of all stakeholders' roles in

### Others

- *Insurers:* Seek timely notification following a cloud incident in order to assess risk and inform coverage. (Similar to government's, cloud providers', and customers' perspectives.)
- *Insurers:* Seek to bound the impact of cloud incidents and limit the scope of their coverage.
- *Insurers:* Want to exclude coverage for certain scenarios (for example, war exclusion) and customers (such

| | | | |
|---|---|---|---|
| managing responses to cloud incidents.[8]<br>• Want to maintain the freedom to leverage and share (as appropriate) incident-related information[9] with involved stakeholders (including foreign governments, if relevant).<br>• Some seek to establish oversight of providers' efforts to prevent future breaches and incidents. | consolidate and standardize incident reporting procedures in order to ascertain that they are efficient and do not impose excessive compliance burdens (including in postincident reporting obligations and other inquiries).<br>• Wish to comply in a timely fashion with legal and reasonable requests in incident coordination and response processes.<br>• Worry that complying with expansive incident disclosure requirements can harm their reputation, erode customer trust, and provoke legal action.<br>• Want to retain the ability to challenge the legality of undesired requests, for forensic or other reporting purposes, via an independent | preventing future incidents. | as, critical infrastructure). |

process (for example, in court).
- Aim to learn from incidents affecting cloud services, including those affecting other providers, in order to prevent future abuses. (Similar to Governments', Customers', and Insurers' perspectives).
- Eager to limit liabilities arising from service disruptions to customers.

## Tensions with Other Cloud Governance Issues

- ***Government Intervention in Extremis, Security and Privacy in Lawful Government Access*** and ***Privacy Protections***: In the event of a major incident, governments may seek to access cloud systems[11] and cloud-hosted data to aid with investigations and recovery. This could affect individual privacy and human rights if it enables governments to access sensitive customer information.

## Potential Ways Ahead

### Government

- Establish mandatory standards for reporting cloud vulnerabilities and incidents that may affect systems critical to the cloud

### Providers

- Proactively identify and define in contracts and/or SLAs roles in incident response and crisis communication vis-à-vis different

### Customers

- Proactively identify and define in contracts and/or SLAs roles in incident response and crisis communication vis-à-vis different

### Others

- *Insurers:* Consider making reporting requirements a condition for coverage.
- *Insurers:* Collaborate in the development of

provider and/or society more broadly. These should enable close-to-real-time situational awareness for all concerned entities.
- Use governmental cloud procurement as leverage to promote cloud services security and robustness and incentivize incident reporting.
- • Clarify expectations and set guardrails for incident response by government, providers, and customers (for example, hack-back, paying ransoms, degree of government access) to help establish a whole-of-system cyber risk management plan.
- Work with cloud providers, customers, insurers, and other key stakeholders to determine appropriate constituencies, documentation, and timelines[12] for disclosures. (Shared with Cloud

cloud incident scenarios.[14] (Shared with Customers.)
- Collaborate in the development of standards to ensure confidentiality in sharing of sensitive incident information. (Shared with Customers and Insurers.)
- Provide timely notification to governments and impacted individuals in the event of a cloud incident. (Shared with Customers.)
- Commit to disclosing information about their own security practices with appropriate government agencies to aid in incident response and recovery coordination internal security practices.
- Work with cloud providers, customers, insurers, credit rating agencies, and other key stakeholders to determine

cloud incident scenarios.[17] (Shared with Cloud Providers.)
- Collaborate in the development of standards to ensure confidentiality in sharing of sensitive incident information. (Shared with Cloud Providers and Insurers.)
- *Enterprise customers:* Work with cloud providers, customers, insurers, credit rating agencies, and pertinent regulators to determine appropriate disclosure constituencies, formats, and timing.[18] (Shared with Governments, Cloud Providers, and Insurers.)
- *Enterprise customers:* Understand and identify their critical functions and dependencies in order to inform the adoption of risk-based approach.

standards to ensure confidentiality in sharing of sensitive incident information. (Shared with cloud providers and customers.)
- *Insurers and credit rating agencies:* Work with cloud providers, customers, and other key stakeholders to determine appropriate disclosure constituencies, documentation, and timelines.[19] (Shared with governments, cloud providers, and customers.)

Providers, Enterprise Customers, Insurers, and Credit Rating Agencies.)
- Consider creating a centralized incident response and reporting office for the cloud sector (in consultation with providers and customers).[13]
- Facilitate cross-agency and cross-industry incident response exercises. (Shared with Cloud Providers and Customers.)

appropriate disclosure constituencies, documentation, and timelines.[15] (Shared with Governments, Customers, Credit Rating Agencies, and Insurers.)
- Perform system penetration and stress tests (potentially also including "bug bounty/white hat hacker" programs) to assist in detection of vulnerabilities and simulation of incident response. (Shared with Governments and Enterprise Customers.)
- Commit to sharing relevant incident information with other cloud providers to assist in the prevention or mitigation of potential spillover across cloud systems.[16]

- *Enterprise customers:* Participate in incident response simulation exercises. (Shared with Governments and Cloud Providers.)

## Recent Examples

- Microsoft Exchange server attack, 2021. For additional information, please see: "Thousands of Microsoft Customers May Have Been Victims of Hack Tied to China." *The New York Times*, March 6, 2021.

- OVH datacenter fire, 2021. For additional information, please see: "Millions of websites offline after fire at French cloud services firm." *Reuters*, March 10, 2021.
- SolarWinds attack, 2020. For additional information, please see: "Suspected Russian hackers spied on U.S. Treasury emails – sources." *Reuters*, December 13, 2020.
- Google cloud outage, 2019. For additional information, please see: "Google details 'catastrophic' cloud outage events: Promises to do better next time." *ZDNet*, June 7, 2019.

## Notes

[1] The word "incidents" is generally understood in the context of cybersecurity, wherein an attack or incidental compromise of systems affects the confidentiality, integrity, and availability of those systems and the data stored, hosted, or processed on them. However, there is a need to account for other, non-malicious triggers of failure, such as natural disasters, which can similarly affect cloud services.

[2] This framework of incident response draws on the Cloud Security Alliance's "Cloud Incident Response (CIR) Framework" and the National Institute of Standards and Technology's "Computer Security Incident Handling Guide". See: CSA, "Cloud Incident Response (CIR) Framework." Cloud Security Alliance (CSA), May 4, 2021, https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/ and NIST, "Computer Security Incident Handling Guide." National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Special Publication 800-61, Revision 2, August 2012, http://dx.doi.org/10.6028/NIST.SP.800-61r2.

[3] See: Lydia Leong, "Multicloud failover is almost always a terrible idea," Gartner, October 14, 2021, https://blogs.gartner.com/lydia_leong/2021/10/14/multicloud-failover-is-almost-always-a-terrible-idea/.

[4] These may include information- and intelligence-sharing arrangements (including cross-border arrangements) between stakeholders which facilitate not just reporting but also detection (especially in the case of multinational corporations).

[5] While the Cybersecurity and Infrastructure Security Agency (CISA) in the U.S. plays this role, not all governments maintain a similar coordinating body. See: CISA, "Cybersecurity and Infrastructure Security Agency," Cybersecurity and Infrastructure Security Agency, n.d., https://www.cisa.gov/.

[6] However, there is debate over whether the "cloud sector" can be considered a coherent and bounded sector for regulatory purposes.

[7] See: CSA, "Cloud Incident Response (CIR) Framework," Cloud Security Alliance (CSA), May 4, 2021, https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/.

[8] For example, as is the case with *Government Intervention in Extremis*, some may seek the authority to assume control over cloud providers or to direct providers to work with government agencies in cases of clear threats to national security.

[9] Including information about the incident's impact on the affected business' mission and finances, as well as technical details, including the types of vulnerabilities exploited and indicators of similar incidents. See: NIST, "Computer Security Incident Handling Guide," National Institute of Standards and Technology (NIST), U.S. Department of Commerce, Special Publication 800-61, Revision 2, August 2012, http://dx.doi.org/10.6028/NIST.SP.800-61r2.

[10] While all customers benefit from insight into an incident and the response of concerned stakeholders, enterprise customers may particularly benefit from transparency and communication, given that contracts for enterprise cloud deployments often place additional security responsibilities on enterprise customers. Whereas consumer cloud offerings are almost entirely managed by the cloud provider.

[11] Governments may wish to exercise significant control over a major cloud provider and direct its recovery efforts following a major cloud incident. For example, the Australian government has expressed that "In an emergency, we see a role for Government to use its enhanced threat picture and unique capabilities to take direct action to protect a critical infrastructure entity or system in the national interest. These powers would be exercised with appropriate immunities and limited by robust checks and balances. The primary purpose of these powers would be to allow Government to assist entities to take technical action to defend and protect their networks and systems" (Emphasis in original.). See: Australian Government, "Protecting Critical Infrastructure and Systems of National Significance," Australian Government, Department of Home Affairs, August 2020, https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf and Australian Government, "Critical Infrastructure – Government assistance in practice," (Diagram) Australian Government, Department of Home Affairs, n.d., https://www.homeaffairs.gov.au/reports-and-pubs/files/ci-government-assistance-in-practice.pdf.

[12] Requirements on disclosure timelines to government agencies vary both within and among nations, with some governments calling for 72-hour timelines and others for as low as 12-hours. These requirements may also vary depending on the function and sectors (such as, critical infrastructure and government services) being served. See: Michael Kans, "Congress Debates Cyber Incident Reporting Deadlines in the NDAA," Just Security, October 26, 2021, https://www.justsecurity.org/78745/congress-debates-cyber-incident-reporting-deadlines-in-the-ndaa/.

[13] While this occurs in the U.S. under the auspices of the Cybersecurity and Infrastructure Security Agency (CISA) and in other individual countries, not all governments maintain a centralized cybersecurity agency to perform this function. See: CISA, "Cybersecurity and Infrastructure Security Agency." Cybersecurity and Infrastructure Security Agency (CISA), n.d., https://www.cisa.gov/.

[14] Cloud providers and their customers should develop and integrate incident notification matrices in their SLAs and/or contracts, laying out each party's responsibilities in crisis communications. For instance, the Cloud Security Alliance sets out the following division of responsibilities for various cloud incident response scenarios: (1) For a security incident occurring in the platform or service layer for a PaaS or SaaS application, the response should be driven by the cloud provider; (2) if a security incident is occurring in the application layer for a PaaS application, the customer should be driving the response; and (3) in the case of a security incident occurring in the platform layer for an IaaS infrastructure cloud, the response should be driven jointly by the customer and the cloud provider to determine if it originated in the customer's environment or the cloud provider's environment. (See: CSA, "Cloud Incident Response (CIR) Framework," Cloud Security Alliance (CSA), May 4, 2021, https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/.) Additionally, the retention of digital forensic evidence should be seen as a shared responsibility. (See: Ben Martini and Kim-Kwang Raymond Choo, "An integrated conceptual digital forensic framework for cloud computing," ScienceDirect, Digital Investigation, vol. 9, issue 2, November 2012, pages 71-80, https://www.sciencedirect.com/science/article/abs/pii/S174228761200059X.)

[15] See: Michael Kans, "Congress Debates Cyber Incident Reporting Deadlines in the NDAA," Just Security, October, 26 2021, https://www.justsecurity.org/78745/congress-debates-cyber-incident-reporting-deadlines-in-the-ndaa/.

[16] This can be achieved through an Information Sharing Analysis Center (ISAC). For example, the Cloud Security Alliance runs the Cloud Cyber Incident Sharing Center (CloudCISC) which facilitates incident data sharing between participating cloud providers. (See: CSA, "CloudCISC," Cloud Security Alliance (CSA), n.d., https://cloudsecurityalliance.org/research/working-groups/cloudcisc/.) In order to be successful, members must participate equally and actively, which requires that they have the willingness and ability to discuss security incidents that have affected their organizations. Participation in these programs by cloud service providers may not be uniform, with some members possibly contributing more actively than others.

[17] Cloud providers and their customers should develop and integrate incident notification matrices in their SLAs and/or contracts, laying out each party's responsibilities in crisis communications. For instance, the Cloud Security Alliance sets out the following division of responsibilities for various cloud incident response scenarios: (1) For a security incident occurring in the platform or service layer for a PaaS or SaaS application, the response should be driven by the cloud provider; (2) if a security incident is occurring in the application layer for a PaaS application, the customer should be driving the response; and (3) in the case of a security incident occurring in the platform layer for an IaaS infrastructure cloud, the response should be driven jointly by the customer and the cloud provider to determine if it originated in the customer's environment or the cloud provider's environment. (See: CSA, "Cloud Incident Response (CIR) Framework," *Cloud Security Alliance (CSA)*, May 4, 2021, https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/.) Additionally, the retention of digital forensic evidence should be seen as a shared responsibility. (See: Ben Martini and Kim-Kwang Raymond Choo, "An integrated conceptual digital forensic framework

for cloud computing," ScienceDirect, Digital Investigation, vol. 9, issue 2, November 2012, pages 71-80, https://www.sciencedirect.com/science/article/abs/pii/S174228761200059X.)

[18] See: Michael Kans, "Congress Debates Cyber Incident Reporting Deadlines in the NDAA," Just Security, October, 26 2021, https://www.justsecurity.org/78745/congress-debates-cyber-incident-reporting-deadlines-in-the-ndaa/.

[19] See: Michael Kans, "Congress Debates Cyber Incident Reporting Deadlines in the NDAA," Just Security, October, 26 2021, https://www.justsecurity.org/78745/congress-debates-cyber-incident-reporting-deadlines-in-the-ndaa/.