CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

Cloud Governance Project
Resilience

Insurance for Cloud Services

Insurance is one of the primary mechanisms for remediating risk events.[1] While (re)insurers recognize the need to expand their cyber insurance offerings as cloud dependence continues to grow rapidly, they nonetheless struggle to assess and bound their exposure to significant cloud incidents and other cyber events, as not all risks can be insured against. Moreover, insurance solutions, even if properly developed for cloud-specific risks, likely will not be sufficient to cover damages that may result from total or widespread service outages, data breaches, and other cloud-related incidents.[2] This situation raises questions about whether, when, and with what scope a government backstop might help mitigate the extent of the harm and help support disaster recovery and remediation activities.[3]

Key Considerations

- ***Insurance may be necessary for remediation activity.*** The high risks to both providers and customers that could materialize as a result of cloud incidents underscore the importance of insurance for risk management and channeling.
- ***Insurers are reluctant to extend coverage.*** Insurers struggle to quantify the potential risks associated with the cloud[4] in particular the likelihood, severity, and financial impact of risk events. As a result, they also struggle to bound their exposure to cascading, cumulative, and potentially cross-border losses triggered by cloud-related incidents (that defy insurance's reliance on risk diversification strategies). This reduces insurers' willingness to extend coverage to cloud-related risks, which is further exacerbated by the growing recognition of the potential systemic risks posed by widespread cloud dependence, wherein an extreme event could trigger simultaneous claims by millions of cloud customers. The potential for such events increases given the cloud market's concentration in the hands of a few hyperscale cloud providers that may be susceptible to common mode failures.
- ***Cloud insurance coverage may prove prohibitively expensive or demanding.*** Insurers may extend coverage only in specific circumstances. They may impose stringent requirements, refuse to cover certain types of events, and lower their overall threshold for coverage in order to bound their exposure to risk. Cloud providers and customers may find that these either diminish the utility of cloud insurance or make useful insurance prohibitively expensive. This would drive down demand for cloud insurance, inhibiting use by customers and providers of an important tool to bolster resilience and manage risk.
- ***Government backstopping and other financial support can make cloud insurance more viable.*** Without a government backstop, cloud providers and customers may not be able to afford the full cost of remediation activities, even if insurance covers some of the expenses. However, there is disagreement among key stakeholders about whether, to what extent, and under what conditions government should serve as the insurer of last resort.

Additionally, some providers and insurers might be concerned that as a condition for backstopping and other support, some governments might demand access to cloud systems and hosted data.

- ***Moral hazard.*** Cloud providers and customers may be incentivized to substitute spending on good risk management for insurance, leading to a problem of "adverse selection," that is, the only cloud providers and customers interested in insurance would be those who cannot/will not manage the risk effectively. Such a circumstance would, in turn, affect how insurers behave. Further, the availability of a government backstopping scheme could itself disincentivize private sector risk management. It could, for example, disincentivize insurers from developing certain cloud insurance products, and lead cloud providers and insurers to adopt riskier postures, confident that they can turn to the government for support.

Stakeholder Perspectives

Government

- Some governments believe that insurance has the potential to enhance cyber risk management, but so far have been disappointed by the combination of limited offerings and modest uptake.
- Wish to ensure that insurance products do not present insolvency risks to carriers.
- Have thus far proved reluctant to provide a safety net for cyber insurance similar to those in place for terrorism insurance.
- Consider national backstopping schemes

Providers

- Want to avoid or at least limit their liability for breaches, service interruptions, data losses, or other incidents.
- Aim to offset risk through affordable insurance products that do not come with onerous requirements attached.
- Encourage governments to offer backstopping arrangements for cyber and cloud catastrophes.
- Might be generally reluctant to discuss their cloud vulnerabilities and risk profiles for fear that it would dissuade cloud

Customers

- Seek affordable comprehensive coverage for their exposure to cloud risks especially those pertaining to business interruption and supply chain risks.

Others

- *Insurers:* Have widely varying appetites to assume risk. Some believe that insurance must respond to the challenge in order to remain relevant to risk in the twenty-first century; others believe that highly connected digital risks carry too much uncertainty and potential for catastrophic losses to be suitable for insurance.
- *Insurers:* Seek visibility into cloud providers' technology and operations to help them understand,

inadequate to address cross-national cyber and cloud risks.
- Resist arrangements that incentivize providers and the private sector to rely on government backstopping; encourage providers and insurers to assume as much responsibility and liability as possible.

adoption and usher in heavy-handed government regulation.

quantify, and bound cloud risks.
- *Insurers:* Want governments to offer a backstopping arrangement for catastrophic cyber and cloud risks differ widely on the desirable parameters of backstopping schemes for these scenarios.
- *Insurers:* However, some insurers and other parties are wary of government intervention in the insurance market and want to preserve the ability to independently determine coverage and set prices.

Tensions with Other Cloud Governance Issues

- ***Effects of Cloud Market Concentration:*** Insurers are hesitant to extend coverage for major cloud incidents because they struggle to quantify the risks associated with such an event. Concentration in the cloud market increases the likelihood that cloud incidents trigger cascading effects across national economies, as customers of all sizes across industries and geographies come to rely on a few hyperscale cloud providers.
- ***Incident Handling Procedures:*** Widespread dependence on the cloud generally makes customers more secure because they are protected by highly skilled security teams at the major cloud service providers, who have a comprehensive view into the threat landscape due to the scale of those cloud providers. This may make insurance coverage of cloud incidents more viable because cloud customers are, on average, more secure than they would be if they were relying solely on their own in-house security teams. However, this

concentration of data means that any compromise of a major cloud provider could lead to a huge number of simultaneous insurance claims.

- ***Government Intervention in Extremis, Security and Privacy in Lawful Government Access, and Privacy Protections:*** Governments may seek to intervene directly in the operations of cloud providers as a condition for backstopping insurers and cloud providers in the event of a major cloud incident. Governments may also or seek greater access to cloud systems and data notwithstanding a major cloud incident, which would implicate the confidentiality of sensitive and personal data.

Potential Ways Ahead

Government

- Facilitate dialogue between government, providers, customers, insurers, and other stakeholders in order to determine and clearly assign liability for cloud service disruptions (including those arising from a sophisticated attack by a nation-state). (Shared with cloud providers, enterprise customers, and insurers.)
- Develop backstopping mechanisms for cloud insurance and cyber insurance markets by drawing on backstopping in other contexts.[5]
- Define conditions for backstopping

Providers

- Collaborate with insurers (and potentially governments) to offer comprehensive coverage for risks emanating from cloud failures.
- Provide insurers with visibility into their cloud technology and operations in order to inform the development of cloud insurance offerings
- Work with governments and insurers to assign concerned stakeholders responsibilities and liabilities in the event of a cloud incident (including a sophisticated attack by a nation-state). (Shared with governments,

Customers

- *Enterprise customers:* Engage in efforts to map their evolving cloud dependency risks and collaborate with insurers to develop cloud insurance. (Shared with insurers.)
- *Enterprise customers:* Help identify the conditions under which government backstopping mechanisms would take effect. (Shared with governments, cloud providers, and insurers.)

Others

- *Insurers:* May require transparency and reporting measures before agreeing to provide coverage.
- *Insurers:* May partner with cloud[6] as well as to drive mainstream adoption of cyber insurance by customers.[7]
- *Insurers:* Establish standards for transparency on customer's economic burden for insurance products.
- *Insurers:* Help develop a common method for assessing the

support to become available (such as the nature and/or scale of the cloud incident). (Shared with cloud providers, enterprise customers, and insurers.)
- Explore other public-private partnerships for mitigating cloud risks.
- Set requirements for cloud providers to ensure data retrievability and bolster the possibility of service continuity in the event of cloud provider or insurer insolvency.

enterprise customers, and insurers.)
- Help identify the conditions under which government backstopping mechanisms would take effect. (Shared with governments, enterprise customers, and insurers.)

cost of business interruption arising through cloud events. (Shared with cloud providers and enterprise customers.)
- *Insurers:* Establish multi-stakeholder dialogues (involving (re)insurers, government, providers, and so on) to increase transparency and understanding around responsibility and accountability in the event of backstopping.
- *Insurers:* Help identify the conditions under which government backstopping mechanisms would take effect. (Shared with governments, cloud providers, and enterprise customers.)

Recent Examples

- Google Cloud's recent partnership with Munich Re and Allianz Global Corporate & Specialty in the development of the "Risk Protection Program" specifically designed for Google Cloud customers. For additional information, see: "Google Cloud, Allianz, Munich Re team up on cyber insurance program," ZDNet, March 2, 2021.
- The U.S. Government Accountability Office has been examining "(1) the risks and costs of cyberattacks on U.S. critical infrastructure; (2) insurance coverage that is available for losses related to cyber risk, including cyberterrorism; and (3) the extent to which TRIP, under the Terrorism Risk Insurance Act (TRIA), is structured to respond to cyberattacks and cyberterrorism." For additional information, see: "Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market," United States Government Accountability Office, May 2021.

Notes

[1] Here, the term "remediation" refers to actions taken beyond restoring service functionality. This could involve, for instance, providing to affected parties financial or in-kind compensation for damages, assurances that the incident has been fully addressed, and taking other actions aimed at remedying the harms caused by an incident and resuming regular operations.

[2] Recognizing that the largest insurance payout for a single event, Hurricane Katrina, amounted to $41 billion, and that the cost of a massive outage to a hyperscale cloud provider could possibly be measured in the trillions, it is unlikely that the insurance industry could bear the economic costs of such an outage. See: Robert P. Hartwig and Claire Wilkinson, Hurricane Katrina: The Five Year Anniversary (New York, NY: Insurance Information Institute, July 2010), https://www.iii.org/sites/default/files/1007Katrina5Anniversary.pdf.

[3] Here, the term "remediation" refers to actions taken beyond restoring service functionality. This could involve, for instance, providing to affected parties financial or in-kind compensation for damages, assurances that the incident has been fully addressed, and taking other actions aimed at remedying the harms caused by an incident and resuming regular operations.

[4] With a 2020 report by Allianz Global Corporate & Specialty noting that cyber claims have grown steadily both in terms of their number and complexity, as threat vectors continuously evolve with the rise of ransomware and nation-state sponsored attacks, as well as "mega" data breaches and drivers of business interruptions. This trend has been exacerbated by the shift to remote work and digitization prompted by the COVID-19 pandemic. See: Allianz Global Corporate & Specialty, Managing the impact of increasing interconnectivity: Trends in cyber risk (Munich, Germany: Allianz SE, March 2021), https://www.agcs.allianz.com/news-and-insights/reports/cyber-risk-trends-2020.html.

[5] For example, in the case of the US, Congress enacted into law the Terrorism Risk Insurance Act, which created a backstop for insurance providers against large-scale, catastrophic losses arising from terrorism-related attacks, outside of the scope of war. Prior to this, insurance companies often used the "war exclusion" in their policies to avoid covering the claims that may arise from terrorist-related acts. See: Jon Bateman, War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions (Washington, DC: Carnegie Endowment for International Peace, October 2020), https://carnegieendowment.org/2020/10/05/war-terrorism-and-catastrophe-in-cyber-insurance-understanding-and-reforming-exclusions-pub-82819 and Aaron Klein and Scott R. Anderson, "A federal backstop for insuring against cyberattacks?" Brookings Institution, September 27, 2019, https://www.brookings.edu/blog/techtank/2019/09/27/a-federal-backstop-for-insuring-against-cyberattacks/.

[6] For example, enabling insurers to connect data to the underwriting process, streamlining applications, and facilitating the continuous monitoring of enterprise insurance customers' security posture over time. See: Larry Dignan, "Google Cloud, Allianz, Munich Re team up on cyber insurance program," ZDNet, March 2, 2021, https://www.zdnet.com/article/google-cloud-allianz-munich-re-team-up-on-cyber-insurance-program/.

[7] With Accenture arguing that online service providers such as Google and Amazon may be better suited to respond the increasing "switching risk" by insurance customers, as technology providers are better positioned to develop more personalized services and innovate in pricing strategies (with 35 percent of respondents to their survey expressing that they would be comfortable with insurance providers accessing their behavioral information in exchange for reduced policy costs). See: Erik J. Sandquist, "Prospering in the switching economy," Accenture, n.d., https://insuranceblog.accenture.com/prospering-in-the-switching-economy.