



The Cloud Challenge: A Multistakeholder Dialogue

ARIEL E. LEVITE

SUMMARY

- Cloud computing represents an increasingly critical platform in the modern, heavily digitized, economy. It affords major benefits to society, but also creates new risks.
- The primary challenge for risk management and insurability of cloud computing is that it presents a complex and systemic exposure. The assessment of vulnerabilities, dependencies, and impacts are all characterized by major uncertainty.
- Cloud service providers (CSPs) are constantly evolving their services, while developing comprehensive risk management strategies. Users are adopting cloud services in diverse and innovative ways, but often find it hard to assess the risks associated with cloud dependence.
- (Re)insurers recognize that they must develop solutions that accurately capture the risk associated with cloud computing. Their appetite to assume the risk is constrained by the high degree of uncertainty, partially driven by the rapidly changing patterns of cloud dependence, and partially caused by CSPs' reticence to share information about their security and robustness practices.
- Regulators are increasing their focus on cloud computing. In the realm of cybersecurity, dependence on third parties represents the most challenging area for regulated entities and regulators to measure risk and develop controls.
- The market concentration of CSPs does present a new, increasingly salient, systemic risk.



The cloud is generating new opportunities for collaboration and is allowing businesses of every size to benefit from world-class cybersecurity. It is also creating a complex risk exposure to both malicious and non-malicious perils, which presents new challenges for governance, risk management, and insurability. Addressing these issues and increasing the availability of (re)insurance for risks connected to the cloud will require collaboration across many different stakeholders.

These were the key findings of a dialogue session convened by CyberCube and the Carnegie Endowment for International Peace, which brought together (re) insurance industry executives, cybersecurity experts, cloud service provider representatives, governmental agencies, and regulators. Some of the organizations that participated in the discussion are listed at the end of this document. The discussions were conducted under Chatham House rules, and the views expressed reflected the personal opinions of the participants and not formal institutional positions.

The “cloud governance challenge” can be characterized by five themes. Research by Carnegie found that “the debate about cloud security remains vague and the public policy implications poorly understood.”¹ The scale and complexity of issues involve a very wide range of interests, which can be in competition with each other. These issues can be grouped in five broad themes:

- Security and robustness
- Resilience
- Consumer protection
- Prosperity, employment, innovation, and sustainability
- Human and civil rights

This dialogue focused on the security, robustness, and resilience themes, in particular the role of (re)insurers and regulators. It is important to note that all three factors are often improved by the adoption of cloud services, as the major CSPs offer superior capabilities and resources for cybersecurity. However, there are serious risk management concerns arising from the aggregation of risk in a small number of CSPs; the opaque nature of security arrangements; and the growing threats (from natural occurrences as well as deliberate action by criminals and states) to cloud services and their supporting infrastructure.

Carnegie suggested that insurance has a significant role to play in the development of governance mechanisms for risks associated with the cloud. However, the systemic nature of the exposure means that some form of public-private partnership may be required in order to develop adequate risk management frameworks. The widespread dependence on the cloud also carries the potential for catastrophic losses, meaning that government “backstop” mechanisms could form part of the solution to encourage greater availability of insurance.

The cloud presents a complex and systemic risk. (Re)insurers and regulators need to assess the potential for severe events affecting the cloud in order to meet solvency and risk management requirements. CyberCube researchers had investigated the potential for severe cloud disruption in order to form the basis of a stress test for an insurance regulator. An outage at a major CSP in 2019 resulted in disruption of services to multiple U.S. regions lasting up to 4.5 hours.² This did not represent a “severe” event for (re)insurance purposes, but the publication of the detail of the event was a great assistance to researchers seeking to improve understanding of the impacts of disruption to the cloud. A severe event could involve cascading impacts from cloud infrastructure to platform-as-a-service and software-as-a-service, which could result in business interruption and data loss across many different sectors.

Users are adopting the cloud in innovative ways, meaning the risk is evolving and multidimensional.

Cloud technology and its usage are constantly evolving; while in the past a CSP would focus solely on its own “technology stack,” today it has to consider a very wide array of services that are dependent on it. As a result, risk management is complex, involving many different functional areas of a CSP and user organizations. As valuable data and services have been transferred to the cloud, so malicious actors have increased their targeting of the cloud for theft, extortion, and espionage. Further threats arise through accidental and physical sources as well as the targeting of the supply chain and supporting infrastructure. This complex and shifting landscape means that risk management and governance require collaboration across multiple stakeholder groups.

(Re)insurers accept the challenge of developing risk transfer solutions for cloud computing.

The cloud is an integral development of the internet, affording immediate and flexible availability of products and services; as such it is essential infrastructure for the modern economy, and insurance must offer risk transfer solutions if it is to remain relevant to risk management. The primary challenge for insurability arises through very complex supply chains where dependencies are hard to identify. The dominance of a small number of CSPs also presents the potential for concentration of exposure and a systemic risk. On the plus side, the use of cloud services generally affords enhanced security compared to on-premises infrastructure.

Insurance has proven to be an effective tool for managing a wide range of risks, and it must rise to the challenge of covering risks associated with the cloud in order to remain relevant. Cyber insurance policies use a definition of computer systems that includes those operated by a third party for the insurer’s benefit. As such the insurer is liable for claims relating to CSPs, exposing the insurer to a huge potential for accumulation of risk. This means that insurers must pay close attention to understanding

their aggregate risk exposure arising through dependence on cloud computing. As a result, they are presently offering only modest coverage for risk associated with cloud dependence. To significantly expand the scope of coverage on offer would require insurers to collectively reduce uncertainty on the potential for severe losses, meaning developing common understanding in partnership with a range of stakeholders.

Regulators are stepping up their efforts to understand the cloud phenomenon, and increasing their scrutiny, but third party dependency is the most challenging aspect of cybersecurity supervision.

For regulators, there is concern that the increasing adoption of the cloud presents more uncertainty for risk management, especially on the nature of dependencies. The complexity and diversity of the arrangements facilitating migration of core business functions to the cloud also thus requires regulators to develop the skills to understand operational aspects associated with cloud dependencies and risk mitigation. Additionally, the dominance of a small number of CSPs also raises the concern regarding concentration of risk. Regulators in different jurisdictions and sectors have introduced a range of measures in order to enforce minimum standards and encourage a risk-based approach to cybersecurity. The management of cyber risk associated with third party providers was identified as the most challenging aspect of regulation for businesses to implement. Small businesses often did not have the resources to supply the required information or assurance, while major technology providers could be inflexible in their approach, unwilling to meet specific requirements of any given client or voluntarily share information required to assess the implications of such dependency. One area of focus going forward could be a requirement for regulated entities to receive assurance of security and robustness standards from third party providers. Such a certification requirement would require agreement on what standards to enforce, which in turn requires collaboration across sectors and professional disciplines.



Conclusion: multidimensional risk requires multidimensional response. The dialogue revealed that stakeholders in (re)insurance and regulation are lagging behind and encountering serious challenges in catching up with the digital and business transformation brought by rapid growth of cloud services. They are struggling to assess and manage the systemic risk exposure arising from the cloud. Collaboration across sectors, for knowledge sharing and the promotion of common standards and best practices, stood out as the recurring theme. Public-private partnerships will be a key element of this collaboration. (Re)insurance must rise to the challenge of providing cover for this complex risk, which will inevitably hinge on the ability of (re)insurers to reduce uncertainty on the potential for severe losses. This, in turn, will mean harnessing the insights of cybersecurity and robustness experts, technology providers, and regulators to create risk management mechanisms that will allow the cloud to achieve its full potential.

NOTES

- 1 Tim Maurer and Garrett Hinck, “Cloud Security: A Primer for Policymakers,” Carnegie Endowment for International Peace, August 31, 2020, <https://carnegieendowment.org/2020/08/31/cloud-security-primer-for-policymakers-pub-82597>.
- 2 “Google Cloud Status Dashboard,” Google, accessed June 5, 2020, <https://status.cloud.google.com/incident/cloud-networking/19009#:~:text=On%20Sunday%202%20June%2C%202019,and%204%20hours%2025%20minutes>.

ACKNOWLEDGMENTS

We wish to acknowledge the contributions of the following organizations. The views expressed in this document do not necessarily reflect the policy of any organization.

Axio
Bermuda Monetary Authority
Carnegie Mellon University
Connecticut Insurance Department
DAC Beachcroft
European Insurance and Occupational Pensions Authority
Guy Carpenter
Hiscox
Israel Ministry of Finance
Israel National Cyber Directorate
Munich Re
New York State Department of Financial Services
Prudential Regulation Authority, Bank of England
Swiss Re



© 2020 Carnegie Endowment for International Peace and CyberCube Analytics Inc. All rights reserved.

Carnegie and CyberCube do not take institutional positions on public policy issues; the views represented herein are those of the author(s) and do not necessarily reflect the views of Carnegie, its staff, or its trustees. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Carnegie Endowment for International Peace and CyberCube Analytics Inc.

Please direct all inquiries to:

Carnegie Endowment for International Peace Publications Department
1779 Massachusetts Avenue NW Washington, DC 20036
P: + 1 202 483 7600
F: + 1 202 483 1840
CarnegieEndowment.org

CyberCube Analytics Inc
58 Maiden Lane
San Francisco
CA 94108
info@cybcube.com
www.cybcube.com