cloud security alliance®

Cloud Concentration Risk and Operational Resilience

PRESENTED BY

Meng-Chow Kang, PhD, CISSP

Associate Professor (Adjunct), NTU, Singapore

Founder and Director, Averitus Pte Ltd

Agenda

1. What is Cloud Concentration Risk?
2. Why is it a concern?
3. Key players/stakeholders' perspectives, actions, and emerging issues
4. Concluding remarks

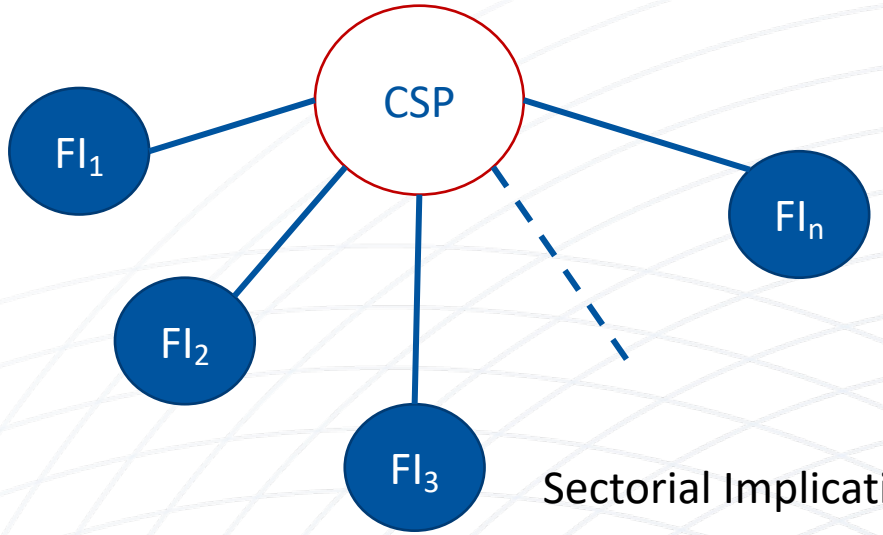
What is Cloud Concentration Risk?

"Macro" concentration risk—can arise in connection with the use by many FIs of the same third-party technology service. The reliance of many FIs on a single service provider may lead to the emergence of a new single point of failure in the financial sector. Harmon, R. , Vytelingum P., and Babaie-Harmon, J., *Cloud Concentration Risk: A Framework Agent Based Model For Systemic Risk Analysis*, Journal of Financial Compliance (Spring 2021).

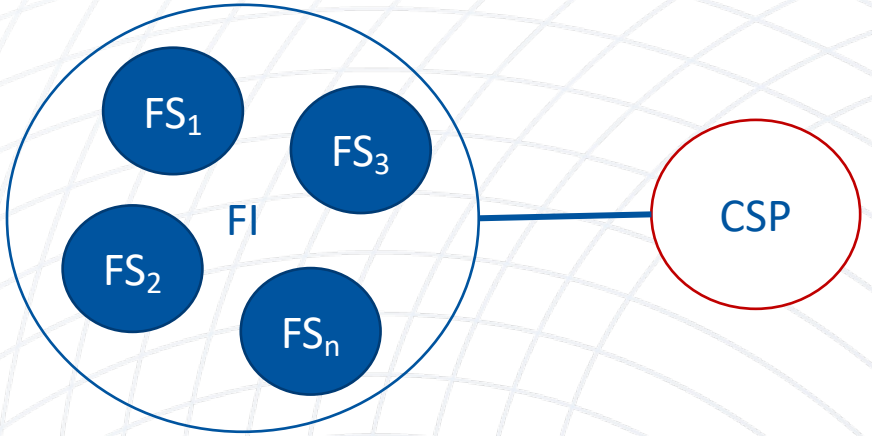
> "Risk arising "when there is concentration of people, technology or other required resources" in the same region or when several of an FI's "critical business services and/or functions are outsourced to a single service provider." – *MAS BCM Guidelines, June 2022*.

Third party concentration risk is defined as (i) when, one provider is handling many financial-related services for the FI and/or (ii) when one provider is providing the same financial-related service to more than one FI and only at the point of disruption where the provider is unable to provide services to the FI as per service levels agreed. – *ABS' Information Paper on Managing Concentration Risk in Third Party Relationships, June 2019.*

> "'ICT concentration risk' means an exposure to individual or multiple related critical ICT third-party service providers creating a degree of dependency on such providers so that the unavailability, failure or other type of shortfall of such provider may potentially endanger the ability of a financial entity to deliver critical or important functions, or cause it to suffer other types of adverse effects, including large losses, or endanger the financial stability of the Union as a whole." – *EU DORA, 2022*

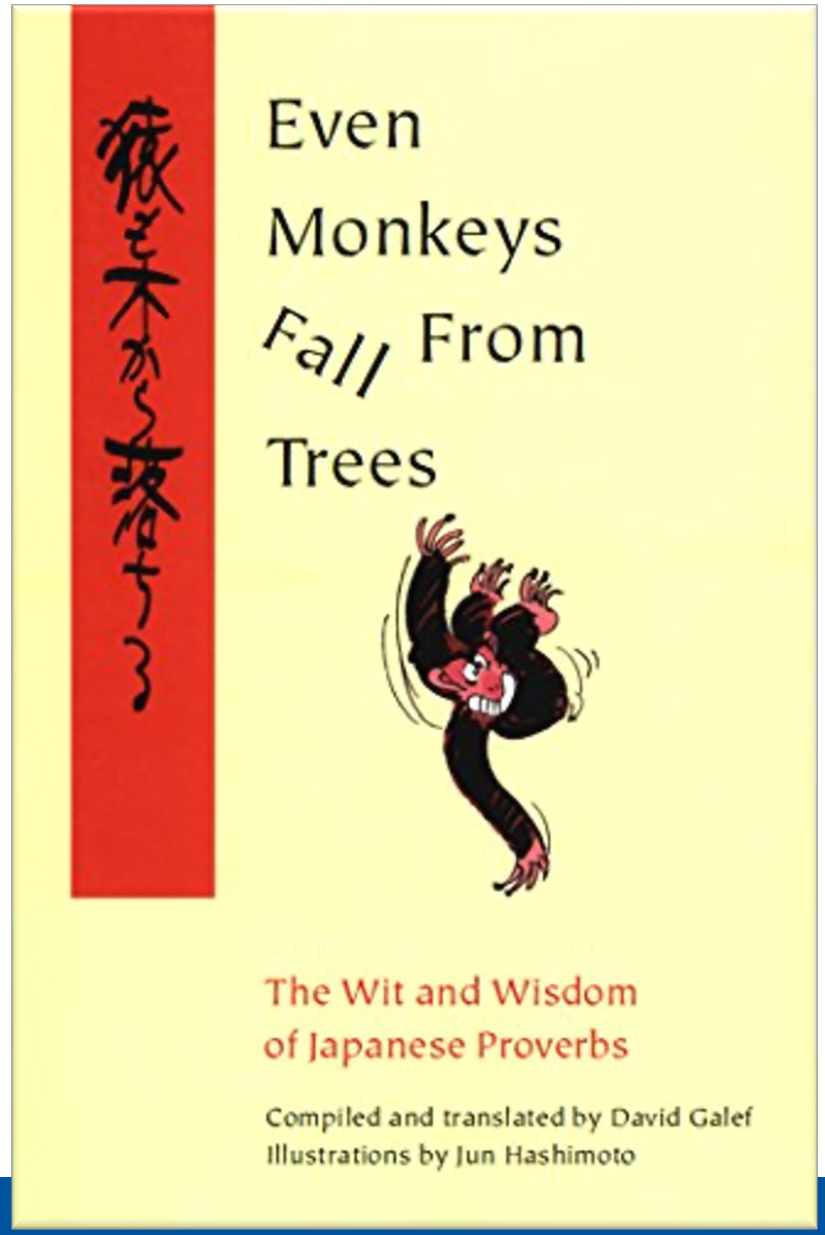


Sectorial Implication



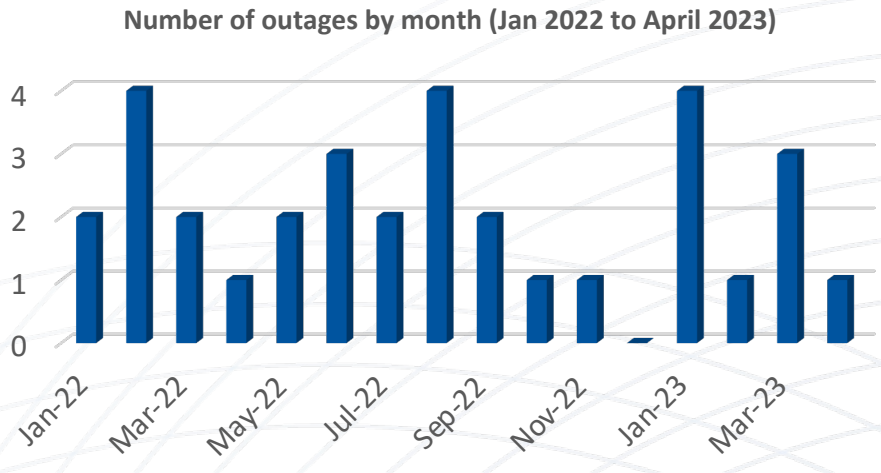
Organizational Implication

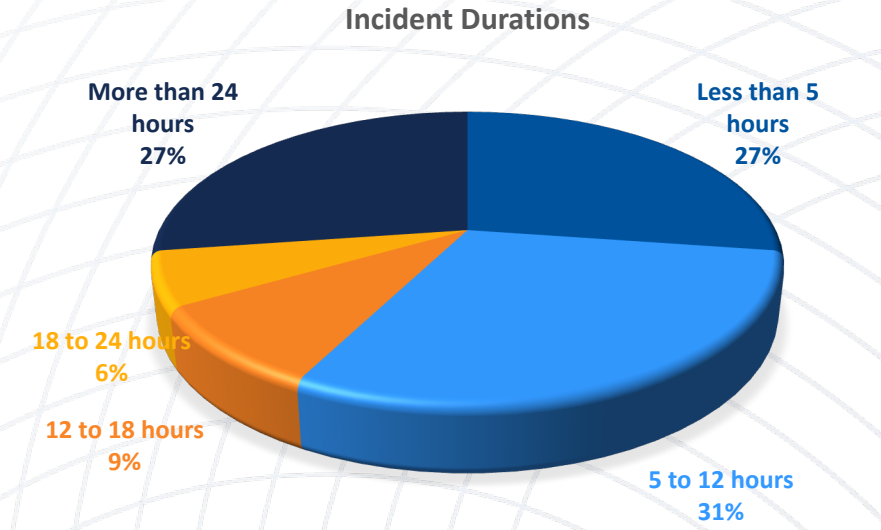
Why is cloud concentration risk a concern?



No perfect system

Date start	Date end	Duration	Incident	Scope of Impact
4/1/22 0:30	5/1/22 7:41	31.18	Azure Cosmos DB - East US connectivity and service availability errors	East US
13/1/22 9:00	14/1/22 20:00	35.00	Azure Resource Manage - Issues with management and resource operations	Global
2/2/22 19:50	2/2/22 22:06	2.27	Azure AD - Service Management Failures	Global
12/2/22 4:38	12/2/22 6:30	1.87	Virtual Machines, Azure SQL, and Storage connection failures	West US
12/2/22 11:45	15/2/22 11:43	71.97	Azure SQL DB and Cosmos DB Unavailable	Six regions
16/2/22 7:31	16/2/22 15:51	8.33	SQL Database and App Service connectivity errors	West Europe
1/3/22 11:49	3/3/22 3:08	39.32	Azure Resource Manager - Service Management Operation Failures	Azure Government Cloud
16/3/22 9:13	16/3/22 10:22	1.15	Azure AD B2C - Authentication Failures and Error Notifications	Global
8/4/22 12:25	9/4/22 14:40	26.25	Service Management Operation Erros Across Azure Services	East US 2 region
30/5/22 9:00	30/5/22 10:24	1.40	Intermittent connectivity issues to Azure Portal - Europe	Europe
31/5/22 21:35	1/6/22 9:54	12.32	Azure Active Directory Sign In logs significant delays in availability	Global
7/6/22 2:41	7/6/22 14:30	11.82	Datacenter cooling event - connectivity issues	East US 2 region
28/6/22 5:26	1/7/22 4:00	70.57	Azure Software Load Balancer failure	Multiple regions
29/6/22 2:46	29/6/22 20:14	17.47	Wide Area Network outage	Multiple regions
21/7/22 3:47	21/7/22 13:30	9.72	SQL Database and SQL Data Warehouse connectivity issues	West Europe
29/7/22 8:00	29/7/22 13:20	5.33	Network connectivity issues	Multiple regions
12/8/22 18:13	13/8/22 3:30	9.28	Azure Communication Services authentication and APIs failures	Multiple regions
18/8/22 16:30	19/8/22 2:22	9.87	Azure Key Vault provisioning failures	Global
27/8/22 2:47	28/8/22 2:00	23.22	Datacenter power event	West US 2
30/8/22 6:00	31/8/22 16:00	34.00	Canonical Ubuntu issue impacted VMs and AKS	Global
7/9/22 9:50	7/9/22 17:21	7.52	Azure Cosmos DB connectivity issues	North Europe
7/9/22 16:10	7/9/22 19:55	3.75	Azure Front Door connectivity issues	Global
26/10/22 0:25	26/10/22 6:00	5.58	Azure Cosmost DB connectivity issues	East US
2/11/22 0:42	3/11/22 5:55	29.22	Encrolling new certificates / provisioning new resources failures	China
18/1/23 9:44	18/1/23 13:10	3.43	Single zone power event	West Europe
23/1/23 15:39	23/1/23 19:38	3.98	Intermittent networking issues	South Central US
25/1/23 7:08	25/1/23 12:43	5.58	Azure networking - Global WAN issues	Global
31/1/23 5:55	1/2/23 0:58	19.05	Service management issues	Ease US 2
7/2/23 20:19	9/2/23 4:30	32.18	Multi-service outage	Asia-Pacific Area
1/3/23 5:25	1/3/23 9:03	3.63	AAD Authentication Issues	China and South East Asia
6/3/23 3:50	6/3/23 17:55	14.08	Azure Storage availability issues	West Europe
23/3/23 2:20	23/3/23 7:30	5.17	Azure Resource Manager - Service Management Operation Failures	West Europe
12/4/23 18:30	12/4/23 22:30	4.00	Network infrastructure - connection failures	Global



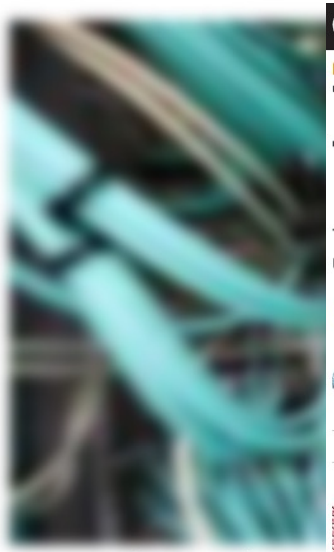


Ref: https://azure.status.microsoft/en-us/status/history/

Cybersecurity failures

Hackers Breach 400,000 UniCredit Bank Accounts for Data

- Bank said to have discovered breaches from 2016 only this week
- Attack comes after 80 Ukrainian lenders compromised in June



Photographer: Chris Ratcliffe/Bloombe

By Sonia Sirletti and Edwar
26 July 2017 at 3:15 pm SGT

CSO ASEAN

FEATURE

The Kaseya ransomware attack: A timeline

REvil's ransomware attack on software provider Kaseya underscored the threats to supply chains that ransomware groups pose. Here is an up-to-date timeline of the attack.

By Michael Hill
UK Editor, CSO | 19 NOVEMBER 2021 18:00 SGT

Security

Hackers exploiting two-year-old VMware flaw to launch large-scale ransomware campaign

Carly Page @carlypage_ / 10:33 PM GMT+8 • February 6, 2023

REUTERS® World Business Legal Markets Breakingviews Technology Inv

Technology

4 minute read · February 4, 2023 1:11 AM GMT+8 · Last Updated 4 days ago

Ransomware attack on data firm ION could take days to fix -sources

By James Pearson and Danilo Masoni

Summary Companies

- Incident could take five days to resolve -source
- ION targeted by Russia-linked ransomware gang Lockbit
- Lockbit says will publish ION data on Saturday
- ABN, Intesa among many likely affected banks

LONDON/MILAN, Feb 2 (Reuters) - A ransomware attack that hit ION Trading UK could take days to fix, leaving scores of brokers unable to process derivatives trades, sources familiar with the matter told Reuters on Thursday.

ION Group, the financial data firm's parent company, said in **a statement** on its website that the attack began on Tuesday.

"The incident is contained to a specific environment, all the affected servers are disconnected, and remediation of services is ongoing," ION Group said, declining

Key players/stakeholders

Industry/Sectorial Regulators

Cloud service providers (CSPs)

Cloud-using organizations (aka., Cloud users)

Industry/Sectorial Regulators

Concerns

- Systemic impact on the industry as a whole
- Effects on public safety and security
- Effects on the economy
- Other implications

Actions

- Beef-up risk management practices of regulated institutions—third-party services, outsourcing, supply chain, and business continuity management
  - Increase supervision and monitoring required of RIs on third-party providers
  - Increase resilience requirements and oversights
- New legislation, e.g., EU's Digital Operational Resilience Act (2022), UK's Proposal to Strengthen Resilience of Critical Third Party (2021)
  - Direct oversight and supervisory authority over critical third-party ICT providers

Emerging Issues

- Compliance overheads to the cloud-using organizations, and service providers
  - How should cross-sectorial authorities coordinate their supervision?
  - What if the requirements conflict between regulators?
- Availability of resources (talents, knowhow, etc.,) to supervise effectively.

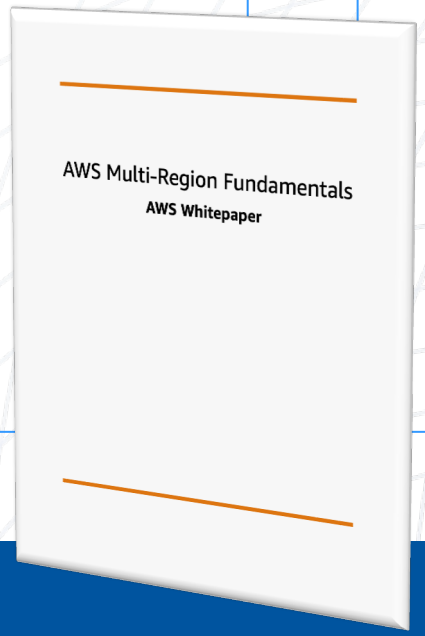
Cloud Service Providers (CSP)

Concerns

- No common agreement amongst major CSPs that cloud is a concentration risk
- Constraints of lower layers' service availability (e.g., SaaS dependency on PaaS and IaaS)
- Over-regulation impacting innovation, increase cost of compliance and services, impact on cloud adoption
- Complexity in compliance arising from different regulators taking different approaches

Actions

- Provision of more services, options, and guidance to cloud using organizations to improve operational resilience
- Geographically increase in service availability footprint—new Region, Local Zones, etc.



Emerging Issues

- Increasing cost of service delivery and assurance
- Increasing cost of cloud adoption/usage.

Cloud users

Concerns

- Definitions and scope of concentration risk
- Uncertainty over risk implications across IaaS, PaaS, and SaaS providers
- Use of cloud is itself a business risk management decision over building more data centers, which has its own risk and concerns, e.g., sustainability/ESG requirements
- Overheads and complexity of compliance

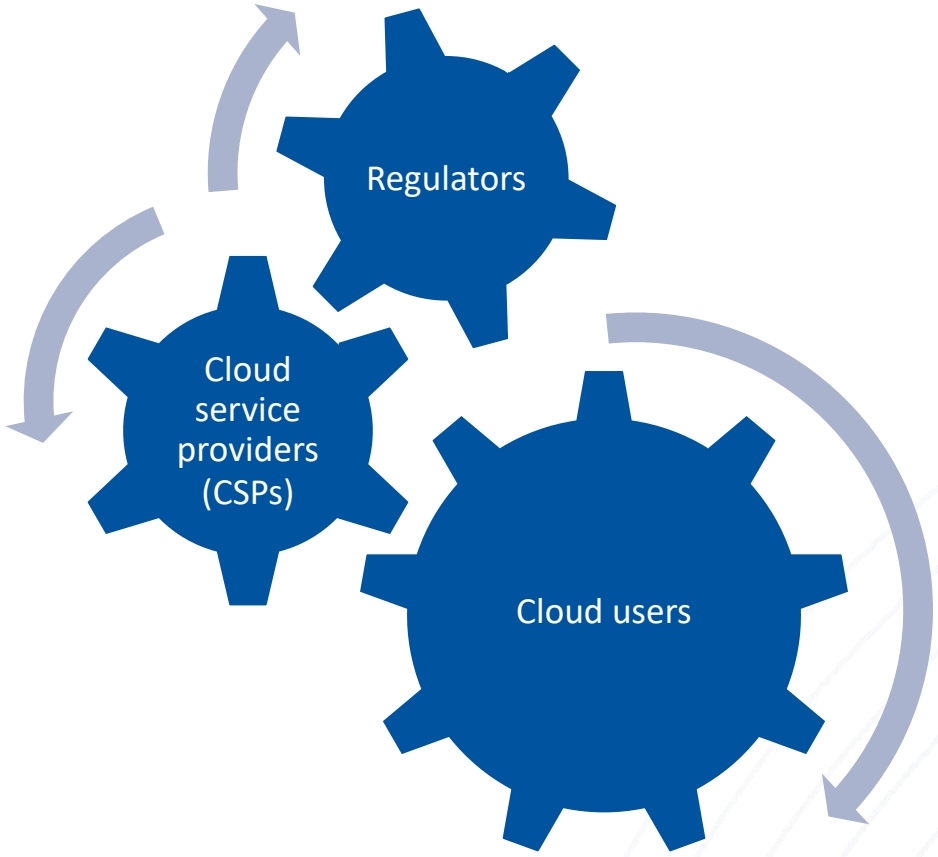
Actions

- Step up on resilience management program
- For those going cloud native, adopt Resilience by Design
- Continue with a hybrid approach– retain critical systems in on-premises data centers, use cloud for newer and non-critical applications
- Attempt on Multi-cloud approach

Emerging Issues

- Increasing complexity and cost in hybrid and multi-cloud approaches
- In a hybrid approach, dependency on on-premises infrastructure increases—by itself may become another concentration risk
- Multi-cloud approach-–limit leverage of cloud innovation. Have to settle on lowest common denominators across CSPs

Concluding remarks



- Relationships among key stakeholders are complex
- Actions of each stakeholders have an impact on the others
- Each stakeholder has a role that affect the risk profile and operational resilience of the other, and the industry as a whole
- Not using cloud services does not eliminate risk either
- Practice Resilience by Design
- Working with CSPs is key for both regulators and cloud users to address or manage their concerns.

Discussion/Q&A

mengchow@LinkedIn