CRC Group
Wholesale & Specialty

State of the Market

Is My Cloud Stack Insured by Cyber Coverage?

Is My Cloud Stack Insured by Cyber Coverage?

In the still evolving area of cyber insurance brokers are constantly being asked to weigh in on issues relating to cyber exposures (severity and susceptibility), risk management practices, insurer appetites, and the direction of the cyber marketplace in general. One such issue is the question of possible insurer aggregation relating to cloud services and Amazon Web Services (AWS) in particular, resulting in a contingent business interruption from a network security event of a customer or supplier.

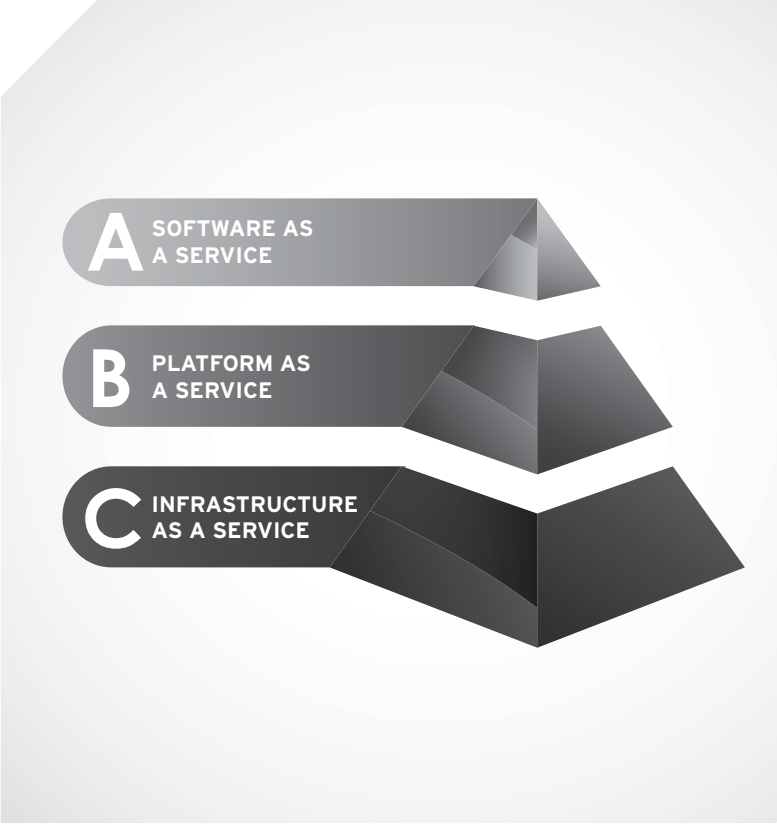
Aggregate limits management for insurance carriers is the idea that a carrier doesn't want to have too many eggs in one basket. For example, for a carrier underwriting property insurance, only insuring properties in Miami-Dade County might be a bad strategy. Carriers want to limit totals, while monitoring their total aggregate exposure and diversifying their portfolio.

In the context of Cyber Insurance, which protects companies for their liability and direct exposures operating in a connected world, aggregation reflects a layered complexity surpassing the relative straightforwardness of geography applicable to other types of coverage, like property insurance. From a regulatory standpoint, the exposure in one state is typically different from another, so cyber insurance written in certain geographical regions might be limited. Additionally, when Target was hacked, retail insureds were quickly subjected to increased underwriting scrutiny and higher pricing. The risk was systemic, and certain industries are logically subject to heightened scrutiny — healthcare, financial institutions.

There is, however, a significant overlay for cyber insurance that relates to the evolution of business models and technology. With the advancement of the cloud stack, SaaS, PaaS, and IaaS – the technological "outsourcing" and sharing of critical company functions – carriers are subjected to a unique level of shared exposure. For example, the 800 pound gorilla, AWS, holds around a 30% market share of cloud infrastructure business[i]. Their clients include everyone from Kellogg's, to the FDA, to Airbnb. If AWS were to be shut down or have a material privacy breach, in theory thousands and thousands of companies may be impacted through the same event.

Insurance carriers are dealing with this exposure in large part through contractual language. Very few carriers directly limit their exposure to AWS by name.

Contingent business interruption losses occur when a service provider, like AWS, stops providing a critical service and the company relying on this service has their business interrupted. Most carriers exclude this loss – suggesting that this liability is really that of the service provider. There are, however, some cyber carriers that will offer this coverage. With more than 40 active cyber insurance carriers, addressing all the specific nuances in coverage for cloud exposures is beyond the scope of this short piece.



Carriers will need to determine if this newer paradigm of shared services in the areas of software, platforms, and infrastructure is something they need to review in their "stack" of aggregation risks. Clients need to understand that carriers are starting to limit coverage for the critical services offered by these providers. Discussion of these issues with carriers and clients will continue as this still nascent 20-year old product continues to evolve.

Endnotes

[i] exhttp://www.businesscloudnews.com/2016/04/29/aws-google-microsoft-and-ibm-pull-away-from-pack-in-race-for-cloud-market-share/ample, AWS

For more information on cyber insurance and risk management, please contact your CRC, CRC Swett or SCU representative.