We are producing our second survey for the year, and the one in this issue is on Cloud Security. When comparing the latest results with our last cloud security survey (July 2019), we see greater adoption of cloud computing, particularly for the SaaS and multi-cloud models. Due to the pandemic, this adoption was stepped up in the last two months, and IT environments became more decentralized and distributed. With much of the workforce now working from home, there is increased dependence on the cloud and cloud services.

The biggest cloud security challenge continues to be “detecting and responding to security incidents in the cloud.” CISOs and CIOs must carefully evaluate the risks posed to the business and deploy the right security tools and controls on the cloud to mitigate those risks.

To learn more about this, I recommend the article in our Viewpoint section titled “Cloud Migration – Security Considerations for Small Businesses,” written by AJ Yawn, who is a Board member of ISC2 and also a cloud security expert. CISOs are being asked to secure remote work environments and small businesses, in particular, are moving to digital models and migrating infrastructure to the cloud, confirms Yawn. Yet, he advises these businesses to understand and evaluate security risks and implications. Read his article to learn about his tips and advice, which also apply to mid- and large enterprises.

I also want to recommend the article “Dancing with the Elephants” in our Insight section. It’s a well-researched article by Raghunath Venkat Thummisi, Founder & CEO of Cannon Cyber. He writes on the dilemma of who is responsible for the security of customer workloads on the cloud. This is also one of the points of contention in our cloud security survey. This can be resolved through the public cloud provider’s shared responsibility model, writes Thummisi. Read more about the shared responsibility model in our Cloud Security survey within this issue.

We hope you enjoy reading the articles in this issue.

Please write to us at editorial@cisomag.com

Jay Bavisi
Editor-in-Chief
Cloud-Ready
Shared Responsibility
TPRM Tips for CISOs

Get Cybersecurity Projects Approved by Articulating the Value of the Data

In the COVID-19 situation, 98% people are working from home and this invites many new risks

Dancing with the Elephants

Cover Story: Security in the Cloud is a Shared Responsibility

Cloud Security Survey

Viewpoint

Cloud Security Companies to Watch

Cloud Security Trends 2020
Reach Global Infosec Community with CISO MAG

1200+ Registered Viewers

70% Average Attendee Engagement

Countries with major registrations:

PAST EVENTS

- May 20, 2020
  CISA and cybersecurity in times of a pandemic
  70% Attendee Engagement

- May 14, 2020
  Back to a new and secure normal
  70% Attendee Engagement

- Apr 30, 2020
  The Superhero CISO

- Apr 21, 2020
  AI - The ultimate weapon in the war against cyber criminals
  70% Attendee Engagement

INTRODUCING YOU THE NEXT LEVEL

VIRTUAL SERIES

To collaborate with us write to:
marketing@cisomag.com

events.cisomag.com

Stats as on May 2020
Engage with Infosec Influencers and Decision makers globally.

REGISTER NOW

events.cisomag.com
Partner with us for CISO MAG Market Trends Report (Data Security) to grow your business and expand your reach.

Inquire Now
Issue Coming Out in September 2020

For Advertising Opportunities write to marketing@cisomag.com

10,000 Global CISOs Will See Your Brand In The Data Security Special Issue
SPECIAL FEATURE

Cloud-Ready
Shared Responsibility
TPRM Tips for CISOs

Becky Swain,
Director of Standards, HITRUST
Third-Party Risk Management (TPRM), commonly referred to as vendor or supply chain risk management, is not a new concept. It was originally founded with a more traditional on-premises IT mindset and was centered on an expectation of always having a significant level of visibility into and control of an organization’s most prised cyber assets; this meant companies asked their most important business partners to share their internal security posture with them.

Then came cloud computing, a catalyst that fundamentally changed how companies do business and consume technology. The cloud, as the epicenter of IT, led to the need for the TPRM model to adapt, necessitating a fundamental change in the mindset to address the emerging risks posed by off-premises cloud-hosted technology services.

Most of the time, it is the obvious 1:1 connection that most organizations consider. They forget the fact that, even though the supply chain by name can be viewed as a “chain,” the growth of technology and the cloud, in particular, have turned this chain into more of a mesh. And, as the saying goes, a chain is only as strong as its weakest link.

The question is, where is that weak link in the mesh? Maybe, more importantly, who owns security and risk management for that link—or links? A change in mindset here involves two primary transformations:

a) A more externally facing view of risk and policy enforcement.

b) A realization that in the cloud, controls are shared with the use of common technology platforms.

As a result, this realization has forced a new “we” rather than an “us vs. them” dialogue with cloud service providers.