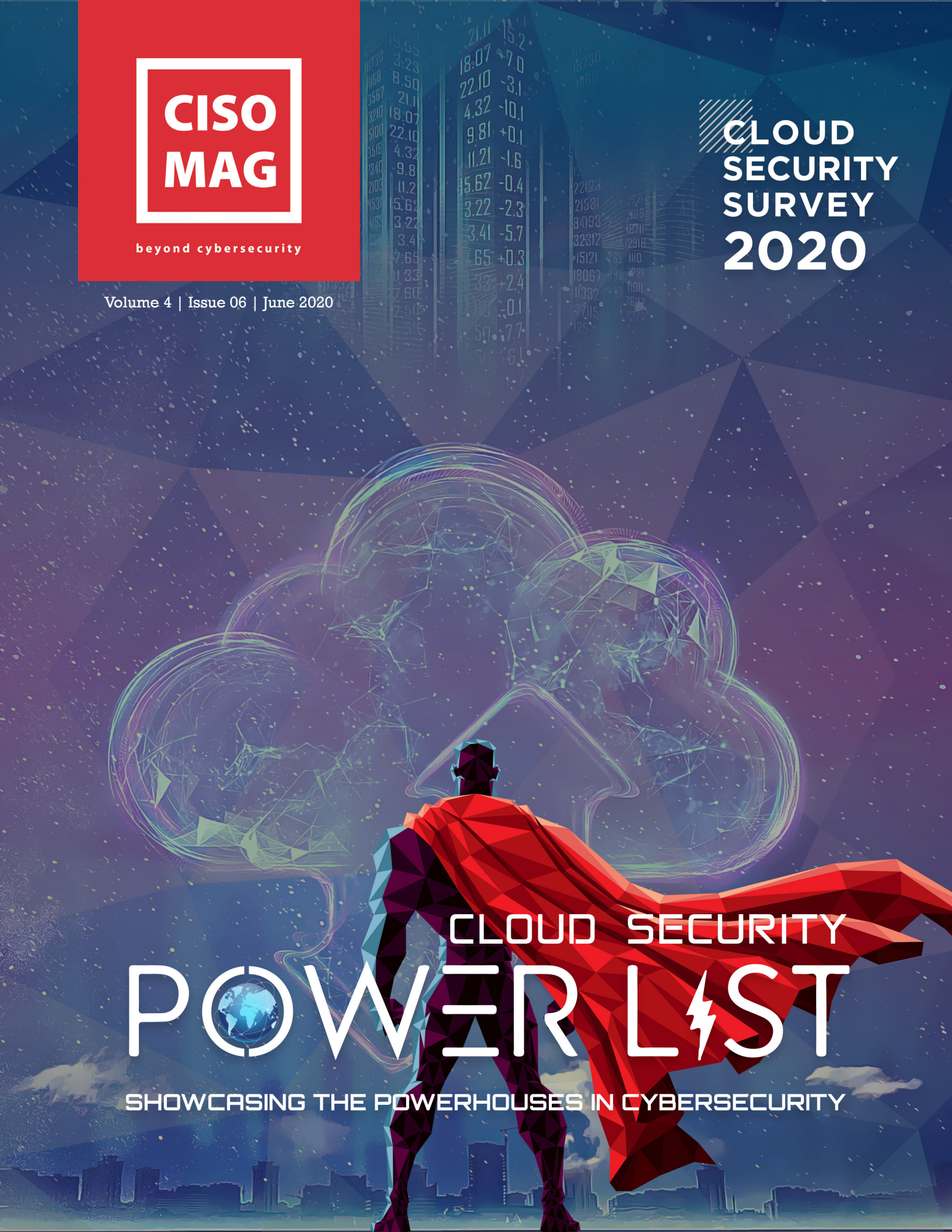
CISO MAG

beyond cybersecurity

Volume 4 | Issue 06 | June 2020

CLOUD SECURITY SURVEY 2020



CLOUD SECURITY POWER LIST

SHOWCASING THE POWERHOUSES IN CYBERSECURITY

CISO MAG
beyond cybersecurity

Volume 4 | Issue 6
June 2020

Image credits: Shutterstock
Cover design, Illustrations, Data visualization & Layouts by: Rajashakher Intha

EDITOR'S NOTE

EVALUATE THE BUSINESS RISKS CAREFULLY BEFORE MOVING TO CLOUD

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 Business**," 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

INDEX

12 SPECIAL FEATURE

Cloud-Ready Shared Responsibility TPRM Tips for CISOs

20 BUZZ...

After the Breach and Beyond

28 UNDER THE SPOTLIGHT

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

40 INSIGHT

Dancing with the Elephants

50 KNOWLEDGE HUB

Get Cybersecurity Projects Approved by Articulating the Value of the Data

58 POWER LIST

Cover Story:
Security in the Cloud is a Shared Responsibility

66 | Cloud Security Survey

82 | Viewpoint

90 | Cloud Security Companies to Watch

CISO MAG RESEARCH REPORT
Cloud Security Trends 2020

CISO MAG
beyond cybersecurity

#CISOMAGLIVE

Reach Global Infosec Community with CISO MAG

1200+
Registered Viewers

70%
Average Attendee Engagement

PAST EVENTS

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

Bryan Ware
CISA,
US Homeland Security

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

Thomas Tschersich
CSO,
Deutsche Telekom AG

Chris Roberts
Researcher, Hacker,
CISO

Apr 30, 2020
The Superhero CISO
95%
Attendee Engagement

Dr. Erdal Ozkaya
CISO at a,
Leading Bank

Apr 21, 2020
AI -The ulimate 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

Countries with major registrations:

Stats as on May 2020

#HyperCyberSec

THE MIDDLE EAST CISO FORUM

June 29, 2020
09:55 AM - 13:00 PM GST

Engage with Infosec Influencers and Decision makers globally.

Dr. Sohail Munir
Advisor - Emerging Technologies And Digital Innovation, Smart Dubai Government

Sultan Altukhaim
Director, Information Security Department (CISO), Risk Management, Capital Market Authority

Dr. Erdal Ozkaya
Managing Director & Regional CISO Standard Chartered Bank (UAE)

Abdullah Biary
CISO
Salama Cooperative Insurance Company

Piyush Kumar Chowhan
Group CIO
Lulu International

Mohamed Mousa
CISO
IKEA, KSA

Thomas Heuckeroth
Group CyberSecurity Lead
Emirates Group

Rasha Abu AlSaud
CISO at a
Leading Bank

Saqib Chaudhry
CISO
Cleveland Clinic Abu Dhabi

REGISTER NOW

events.cisomag.com

Market Trends Report
(Data Security)

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

SPECIAL FEATURE

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 prized 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.

At first, these conversations were uncomfortable, if non-existent. Therefore, this realization and related mind shift did not happen overnight. It took two key changes in industry trends to start the TPRM-in-the-cloud journey that finally got us to where we are today:

The democratization and consumerism of IT—With the birth of the cloud—and its ease of accessibility and consumption—emerged a new "shadow-IT" developer community which was no longer bogged down by the traditional, enterprise IT, process-heavy red tape. With the shadow IT approach, developers bypassed all the existing enterprise security controls baked into those processes.

In turn, this renewed sense of empowerment enabled developers to accelerate their time-to-market. They could also deliver new, innovative solutions to keep pace with an emerging competitive landscape of technology service providers that demanded increased shareholder value and revenue growth.

From the TPRM perspective, this became problematic when customers sought answers to their supplier risk due-diligence questionnaires. But no one within the enterprise IT function could respond, as had been the prior modus operandi.

This forced CISOs—along with their CIO partners—to redefine their cross-functional engagement model to strengthen their partnerships with the company's lines of business and associated product teams. They did this in hopes of building a similar partnership to the one they had previously nurtured with their enterprise IT counterparts. Further, it accompanied the new addition to the company's set of most prized cyber assets: customer data.

With this new supply chain risk perspective on customer data protection—along with the expansion of global privacy regulation—there emerged a number of security and privacy industry standards and

fied compliance control frameworks. These frameworks were more suitable for addressing the cloud security risks that CISOs would need to adopt and integrate into their information security and governance, risk, and compliance (GRC) programs. The frameworks also helped CISOs safeguard and appropriately manage both their own supply chain risks and the supply chains of their customers.

Technology innovation and cloud supply chain ecosystem complexities—With the promise of the cloud came the next big innovation and a new term added to our tech-savvy vernacular: "Big Data." Since then, there have been significant advancements in the types of technology solutions commonly used by consumers and businesses today—with further growth expected to continue in the future—e.g., artificial intelligence (AI), robotics, and the Internet-of-Things (IoT), to name a few.

These advancements have resulted in the creation of a vast and complex ecosystem of cloud service providers, solution partners, and consumers. They all share a common cloud platform, characterized by a comingled and integrated set of varying types of technologies, which are primarily hosted off-premises—e.g., web and mobile applications that are hosted on highly-scalable virtual infrastructures.

the CISO's quality of ex-