



beyond cybersecurity

Volume 3 | Issue 6 | June 2019

CISO THE TECHNICAL UNICORN

PROVISE FOR YOU

- ProVise is an Independent, product agnostic research driven Advisory firm specializing in GRC and Cyber Security Professional Services.
- What started with two people in 2011 is now an entity spanning across regions with a global portfolio of leading customers.
- Since its inception in 2011, ProVise has expanded its footprint in 7 countries and has around 175+ Successful projects executed.
- As of today, ProVise is a Trusted cyber security partner in UAE for the Largest Police Force, Largest Real Estate Firm, Largest Telecom Company, Largest Entertainment Island and striving for much more.

OUR BUSINESS LINES



Technology Governance, Risk and Compliance advisory business

- WINNING IS NOW A HABIT IN PROVISE



Industry specific , Threat Centric Cyber Security Assurance and Monitoring

- R&D IS THE CORE OF ALL SERVICES AND PROJECTS



Product Engineering and R&D is located in Bengaluru.

- GRC COGNITIVE PLATFORM • CYBER SECURITY PLATFORM

OUR DNA

Dream is not that which you see while sleeping, it is something that does not let you sleep.

Vision
 To be the customers partner of choice for safeguarding their digital assets



innovation distinguishes between a leader and a follower

Mission 2021

- Top 3 Cyber Security Research Firms in Asia
- No.1 GRC Platform Globally
- No.1 GRC Consulting Firm Globally

08
BUZZ
When It Comes to Endpoint Security,
We Are All Fighting the Same Battles

16
UNDER THE SPOTLIGHT
Asaf Lifshitz,
Co-Founder and CEO of Sayata Labs

26
COVER STORY
CISO: The Technical Unicorn

38
COLLABORATIONS
InfoSec Partnerships

48
IN THE NEWS
Top Stories from
the Cybersecurity World

54
IN THE HOTSEAT
High-Profile Appointments in the
Cybersecurity World

60
KICKSTARTERS
Startups Making Waves in the
Cybersecurity World



08



16



26



38



48



54



60



EDITOR'S NOTE

The role of a CISO is evolving at a faster pace than ever before. From a leader who was responsible for an organization's information and data security to someone who has moved up the ladder to become a business enabler, CISO is the modern-day unicorn in theory. A good CISO identifies and translates complex technical security risks to the business and has the capability to provide tactical solutions with a business minded approach. Our Cover Story dives deeper into the role of CISO and how it has evolved into a force to be reckoned with.

In our Under the Spotlight section, we interview Asaf Lifshitz, Co-Founder and CEO of Sayata Labs. During the interaction, Asaf talks comprehensively about his journey, the challenges he faced while starting Sayata Labs, and what are the crucial elements in assessing a company's risk exposure. Move to our Buzz section where Brian Madden, lead field technologist, End-User Computing, VMware, talks about the battles of endpoint security.

Tell us what you think of this issue. If you have any suggestions, comments or queries, please reach us at editorial@cisomag.com.

Jay Bavisi
Editor-in-Chief

**CISO
MAG**

beyond cybersecurity

Volume 3 | Issue 6
June 2019

Editorial
International Editor
Amber Pedroncelli
amber.pedroncelli@eccouncil.org

Principal Editor
Rahul Arora
rahul.arora@eccouncil.org

Senior Feature Writer
Augustin Kurian
augustin.k@eccouncil.org

Feature Writer
Rudra Srinivas
rudra.s@eccouncil.org

Media and Design
Media Director
Saba Mohammad
saba.mohammad@eccouncil.org

Sr. Graphics Designer
Sameer Surve
sameer.s@eccouncil.org

UI/UX Designer
Rajashakher Intha
rajashakher.i@eccouncil.org

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

Senior Director,
Compliance & Governance
Cherylann Vanderhide
cherylann@eccouncil.org

Deputy Business Head
Jyoti Punjabi
jyoti.punjabi@eccouncil.org

Marketing and Business Development
Officer
Riddhi Chandra
riddhi.c@eccouncil.org

Digital Marketing Manager
Jiten Waghela
jiten.w@eccouncil.org

Publishing Sales Manager
Taruna Bose
taruna.b@eccouncil.org

Technology
Director of Technology
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd., Editor: Rahul Arora. The publishers regret that they cannot accept liability for errors & omissions contained in this publication, howsoever caused. The opinion & views contained in this publication are not necessarily those of the publisher. Readers are advised to seek specialist advice before acting on the information contained in the publication which is provided for general use & may not be appropriate for the readers' particular circumstances. The ownership of trade marks is acknowledged. No part of this publication or any part of the contents thereof may be reproduced, stored in a retrieval system, or transmitted in any form without the permission of the publishers in writing.



POWER LIST

SHOWCASING THE POWERHOUSES IN CYBERSECURITY

FOR MORE DETAILS:

JYOTI PUNJABI

Deputy Business Head - CISO MAG

☎ +91 9963654422

✉ jyoti.punjabi@eccouncil.org

TARUNA BOSE


Publishing Sales Manager - CISO MAG

☎ +91 7838483171

✉ taruna.b@eccouncil.org

When It Comes to Endpoint Security, We Are All Fighting the Same Battles

Brian Madden, Lead Field Technologist,
End-User Computing, VMware

A woman with long dark hair and glasses, wearing a white blazer, is looking down at a tablet she is holding. She is in a server room with blue lighting and server racks in the background.

I joined VMware a little over a year ago and since then, I've traveled to 18 countries and 26 U.S. states to meet with over 160 current and prospective customers. During these customer visits, I listen to their end user computing plans and strategy, explain VMware's vision and product roadmap, and discuss how those two might align. The most surprising thing to me after all these meetings is how similar most customers are, particularly when it comes to their most pressing end user computing challenges.

I know this goes against everything we learn from Dale Carnegie or from Sales Training 101 - "Make every customer feel special!" and "Each customer is a unique snowflake!" While every customer and conversation is indeed unique, I've found that every customer is more or less fighting the same battles when it comes to locking down devices, apps and data. Here are my top three observations:

Battle #1: A Dissolving Security Perimeter

Do you remember the days when every employee came into the office, logged into a stationary device that was connected to the corporate network, and IT could definitively identify the security perimeter? Those days are far behind us as employees demand to work from anywhere, including from locations outside of areas where IT has control. Employees also want to access

apps and data from a variety of devices, even if IT doesn't "own" them.

As the number of devices accessing corporate data grows, IT faces an expanding security perimeter problem which in turn results in a larger attack surface.

To address this, many companies are adopting a "Zero Trust" approach. Put simply, Zero Trust means that all sources attempting to access company data - either from inside or outside a secure company network - must continuously be verified. This "never trust, always verify" mentality ensures the right people have the right level of access to the right resources and in the right context.

While there is no silver bullet when it comes to achieving a Zero Trust security architecture, identity, access, and device management are the core technologies that organizations should start with on their journeys. By implementing these technologies as part of a broader security architecture, IT can verify user identity and device compliance as individuals access company resources irrespective of their physical location.

Battle #2: If Security Policy Diminishes Experience, Employees Will Go Rogue

No matter what security approach IT takes, it must not (but oftentimes does) get in the way of employees'

digital experience. As they search for corporate security perimeter breaches, typical IT responses and policy is to block applications access, which in turn obstructs employee experience and productivity. This will not work.

The simple truth is that if IT doesn't let the employee work in the way they want, employees will find a way to circumvent security tools and processes, putting the organization at even greater risk.

Ultimate security-conscious research has demonstrated a direct correlation between providing employees with a positive digital experience (i.e., secure device flexibility, seamless access to apps, secure work regulations) and an organization's competitive position, revenue growth and employee retention. In short, there is a lot on the line when it comes to making sure your security strategy goes with employee experience.

Again, back to the Zero Trust doctrine. With the right architecture in place that puts employee-friendly policies back at the center, IT teams can strike a balance between enterprise security and employee experience. Identity verification, for example, is something employees are used to with the advent of biometric and facial recognition security technology. When leveraged to protect company information, the overall experience becomes more natural, seamless, and intuitive for employees while also providing IT with the measures they need when it comes to security. Win-win.

SUBSCRIBE NOW
FOR COMPLETE ISSUE