



**CISO  
MAG**

beyond cybersecurity

Volume 4 | Issue 10 | October 2020



# SECURING APPLICATIONS

## IN A BORDERLESS WORLD

**All-New C|EH**  
Certified Ethical Hacker

v11

# The Ultimate Ethical Hacking Certification

Demanded by **Employers**. Respected by **Peers**.

**Get Certified Today**







Volume 4 | Issue 10  
October 2020

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

Principal Editor  
**Brian Pereira**  
brian.p@eccouncil.org

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

Feature Writer  
**Rudra Srinivas**  
rudra.s@eccouncil.org

Technical Writer  
**Mihir Bagwe**  
mihir.b@eccouncil.org

Feature Writer  
**Pooja Tikekar**  
pooja.v@eccouncil.org

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

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

Management  
Executive Director  
**Apoorba Kumar\***  
apoorba@eccouncil.org

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

Head of Marketing  
**Deepali Mistry**  
deepali.m@eccouncil.org

Marketing Manager  
**Riddhi Chandra**  
riddhi.c@eccouncil.org

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

International Sponsorship Manager  
**Mir Ali Asgher Abedi**  
mir.ali@eccouncil.org

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

Publishing Sales Manager  
**Vaishali Jain**  
vaishali.j@eccouncil.org

Executive – Marketing and Operations  
**Munazza Khan**  
munazza.k@eccouncil.org

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

EDITOR'S NOTE

SHIFT LEFT TO MAKE APPLICATIONS SECURE

I am distressed to read about the millions of blue collar and construction workers, mechanics, and other low-skill workers who lost their jobs in the past few months. Even highly educated people in the travel, hospitality, entertainment, and other sectors are out of work. And yet, you and I still have jobs and can work from the comfort of our homes. Knowledge workers who used to work in an office can continue performing their duties from home – all thanks to the Internet. They can access all the computing resources they need for work. Applications are the core or the conduit to services and data on the Internet.

On the infrastructure front, delivery models are changing. Everything is now being offered “as-a-service” with increased virtualization of physical infrastructure. Even laptops and desktops are being virtualized through VDI and DaaS (desktop-as-service).

Bad actors are now focusing on Applications to get into enterprise networks via endpoints. Downloading a malicious app on your smartphone could potentially threaten security if the device is connected to the enterprise network. That's also applicable to other endpoints like laptops, browsers (malicious extensions and malicious scripts), and tablets.

Therefore, putting the organization's applications first will become a strategic move to safeguard the business's most valued assets, writes Vishak Raman, Director, Security Business, Cisco India & SAARC. And you can read his article, which is our cover story on page 58.

But how do we make applications secure?

Application Security should not be an afterthought. Developers need to think about application security at the beginning of the development cycle. CISOs like to talk about “Security by Design” and adopting the DevSecOps or SecOps model. Development and security teams should work together and review each other's progress throughout the application development cycle. Testing and fixing bugs must happen from the rollout of the first “alpha” versions. Developers are expected to have basic application security training – basic understanding in input validation, error handling, and secure data handling when they write code.

That's the kind of transformation and culture that's needed in an organization to make applications more secure.

Now it's time to Shift Left and adopt the DevSecOps model for application development.

Our next issue will be on **Compliance**. To participate, do write to me at either of the email addresses below.

We hope you enjoy reading all the other articles in this issue as well.

Please write to us at [editorial@cisomag.com](mailto:editorial@cisomag.com) or [cisomag@eccouncil.org](mailto:cisomag@eccouncil.org)

Jay Bavisi  
Editor-in-Chief



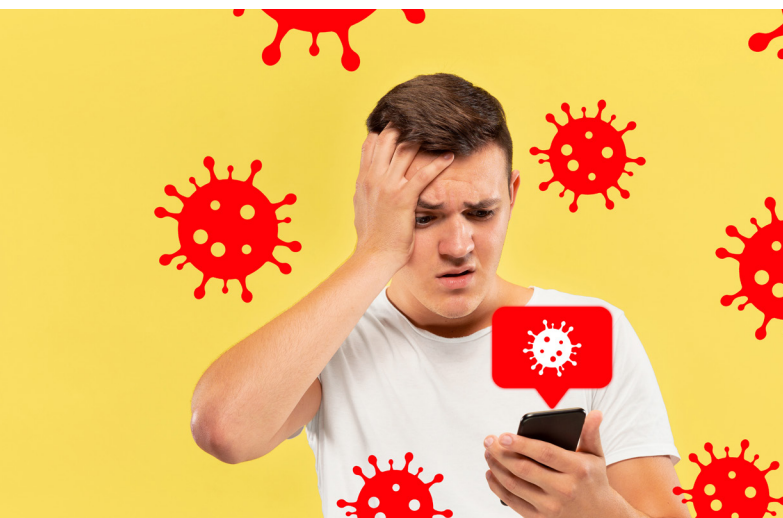
Image credits: Shutterstock  
Cover & Layouts by: Rajashakher Intha

\* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd., Editor: Brian Pereira. 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 & SEPTEMBER 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 SEPTEMBER be reproduced, stored in a retrieval system, or transmitted in any form without the permission of the publishers in writing.



## 10 | **BUZZ**

How COVID-19 has Affected the Application Security Space



## 28 | **INSIGHT**

The Role of a CISO in Ensuring Application Security for Employees



## 38 | **TABLE TALK**

Locking down access is not the answer, but controlling and understanding data is, says Laurence Pitt, Global Security Strategy Director, Juniper Networks



## 18 | **UNDER THE SPOTLIGHT**

Yotam Gutman, Marketing Director, Sentinel One: Attackers are looking to break into your organization either by a broken VPN or RDP protocols



## 48 | **KNOWLEDGE HUB**

Data Protection Sustainability  
A Self Compensating System



## 68 | **VIEWPOINT**

The Last 11 Email Accounts You'll Ever Need

## 78 | **REWIND** <<

Top Newsmakers and the Hottest Cybersecurity News of the Month



## 58 | **COVER STORY**

Leading Post-COVID –  
Securing Applications in  
a Borderless World







# THE AUSTRALIA CISO CONFLUENCE

October 28 & 29  
2020

CYBERSECURITY  
IN A HYPER CONNECTED  
ECOSYSTEM

REGISTRATIONS OPEN

TOP INFOSEC  
LEADERS  
OF **AUSTRALIA**  
AT ONE  
PLATFORM

AN **EC-COUNCIL** INITIATIVE

To partner with us write to: [cisomag@eccouncil.org](mailto:cisomag@eccouncil.org)

 [events.cisomag.com](https://events.cisomag.com)

#HyperCyberSec  
#AUCISOCon  
#CISOMAGLIVE



# HOW COVID-19 HAS AFFECTED THE APPLICATION SECURITY SPACE



**Rohan Vaidya**

Regional Director of Sales – India  
**CyberArk**





**W**hen the COVID-19 pandemic hit, all businesses were shaken awake by the rapid transmission of this virus. The disruption it unleashed on the global economy was beyond anyone's comprehension. As they developed overnight responses to ensure business continuity, many were left vulnerable and exposed to security breaches. Amidst the pandemic, while most people work from home, cybercriminals have upped the ante and are not taking any time off. With many employees working remotely and organizations shifting their focus to their employees' health and safety, security and risk management

teams need to be more vigilant than ever before. There is a need for eternal vigilance.

The pandemic has impacted industries in several ways:

#### 1. Risks from Self-service Applications

The deployment of self-service applications has become *de rigueur*. Organizations have rationalized help desks to save time and labor. End-users reset passwords and unlock their accounts. They may use multi-factor authentication. It enables them to access apps and other services without adding load to the help desk.

#### 2. Impact on Third-party Vendors

Just-in-time provisioning for third-party vendors while looking to mobilize the workforce has increased the number of third-party users. These users are a new challenge since they are outside the company directory and their access could be problematic. The attack surface can be reduced through solutions that allow and block access through self-service onboarding. Hence, vendors can get the right access and just the right amount of manual intervention to allow or

**SUBSCRIBE NOW**

**TO READ THE FULL ISSUE**