

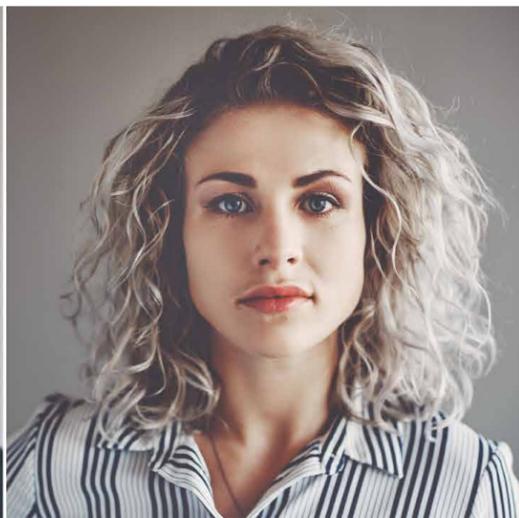
A person in a dark, hooded outfit stands in a cave, looking towards a large, glowing digital network map overlaid on the cave walls. The map consists of yellow nodes and connecting lines, with some nodes highlighted by orange circles. The person is holding a device in their right hand. The overall atmosphere is dark and mysterious, with a focus on digital security and network infrastructure.

**CISO
MAG**

beyond cybersecurity

Volume 2 | Issue 5 | June 2018

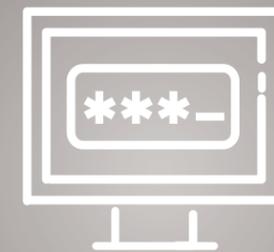
BUILDING WALLS WHILE LEAVING THE DOORS OPEN



What you know.



Who you are.



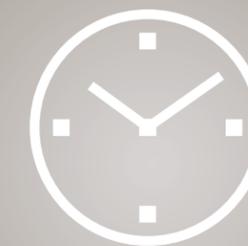
What you have.



What you do.



Where you are.



When you act.

You've got a variety of users.

We've got a variety of authentication factors.

What's Your DigitalPersona®?

Try DigitalPersona for free and discover the difference.

crossmatch.com/dpdifference



INDEX



16



24



36



56



EDITOR'S NOTE

Cyber attacks on applications make up a larger percentage of all attacks than all other types combined. To be precise, 84 percent of all cyber attacks occur on applications, which is far more than network attacks. Yet, network attacks continue to get the most attention. In this issue, we focus on application security and how a few minor developer mistakes can create huge vulnerabilities in the applications. We have a piece by Lee Carsten that addresses things that CISOs get wrong about AppSec, and how AppSec has evolved since the early days of OWASP.

In Under the Spotlight, we interview Jimmy Sanders, President of ISSA San Francisco, who speaks about application security, diversity in security, the most impactful breaches in recent history, and more. He also speaks about improving diversity in the information security space and how several degree programs are paving the way toward its betterment. We also interview Vishal Salvi, CISO of Infosys, who talks about his journey, the evolving role of CISOs, application security, and using blockchain technology to secure the banking sector. Our Insight section features Sebastian Hess writing about cyber insurance essentials and risk management.

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

BUZZ 8
What CISOs get Wrong About AppSec

COVER STORY 16
Building Walls while Leaving the Doors Open

UNDER THE SPOTLIGHT 24
Jimmy Sanders
President of ISSA San Francisco

INSIGHT 36
Cyber Insurance Paper: The Essentials

COLLABORATIONS 48
Infosec Partnerships

TABLE TALK 56
Vishal Salvi
Chief Information Security Officer, Infosys

IN THE NEWS 62
Top Stories from the Cybersecurity World

IN THE HOTSEAT 68
High-Profile Appointments in the Cybersecurity World

KICKSTARTERS 72
Startups Making Waves in the Cybersecurity World

CISO MAG

beyond cybersecurity

Volume 2 | Issue 5
June 2018

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

Senior Editor
Rahul Arora
rahul.arora@eccouncil.org

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

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

Design Head and Visualizer
MSH Rabbani
rabbani@eccouncil.org

Designer
Jeevana Rao Jinaga
jeevana.j@eccouncil.org

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

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

Marketing & Sales
General Manager
Meghana Vyas
meghana.vyas@eccouncil.org

Marketing Manager
Pooja Saga
pooja.saga@eccouncil.org

Sales Manager - India
Basant Das
basant.das@eccouncil.org

Sales Manager - North America
Jessica Johnson
jessica.johnson@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.



ASEAN

Cyber Security Summit

EC-Council

17th August 2018
Singapore

Building a resilient and innovative **ASEAN**

OUR SPEAKERS



Dato' Dr. Haji Amirudin Bin Abdul Wahab
Chief Executive Officer (CEO)
Cyber Security Malaysia



Vincent Loy
Managing Director
Accenture



May-Ann Lim
Managing Director
Asia Cloud Computing Association



Hock Lai Chia
President
Singapore Fintech Association,
Singapore



Dr. Rudi Lumanto
Chairman
Indonesia Security Incident Response Team
on Internet Infrastructure, Indonesia



Malikkhan Kotadia
Mentor
The FinLab Pte Ltd, Singapore



Mark Johnston
Customer Engineer - Security (JAPAC)
Google Cloud



Prof. Lam Kwok Yan
Professor of Computer Science,
School of Computer Science and
Engineering
Nanyang Technological University

Contact

Marketing Manager
Rakesh Acharya
rakesh.acharya@eccouncil.org
+91-79778-28905

OUR PARTNERS

Platinum Partner



Gold Partner



Silver Partner



Startup Partner



Supporting Partner



Supporting Associations



Education Partner



Exclusive Media Partner



Media Partners



What CISOs get wrong about APPSEC

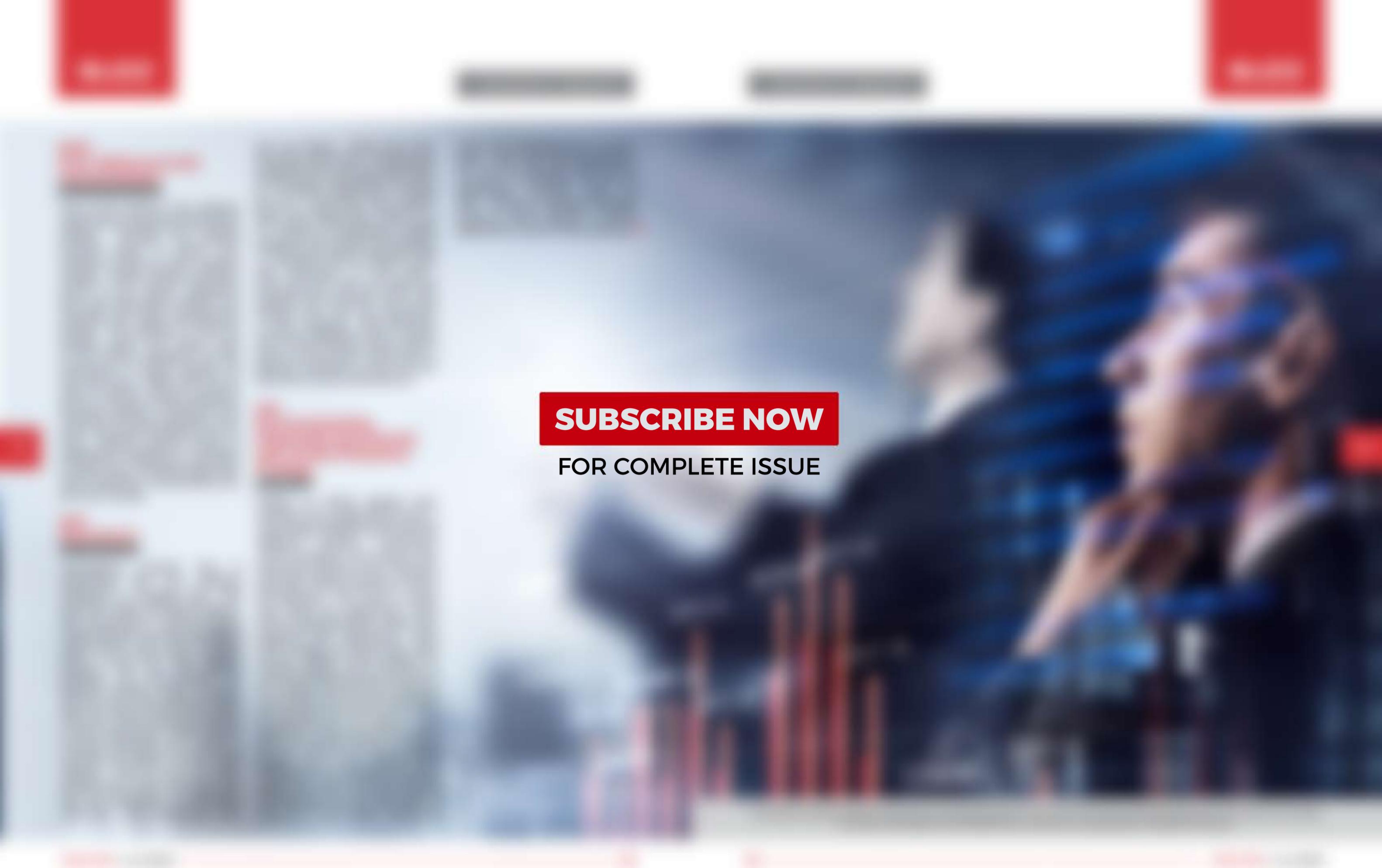
Lee Carsten



Application security has matured quite a bit since the early days of OWASP. The pace of software development is growing exponentially, and the industry is doing all it can to keep up. Here are some of the areas I have seen that can get you into trouble if you aren't paying close attention.

Lack of visibility into what you own

Coverage is a key component of any application security program. It is typical for a modern enterprise to have 2-4 times as many applications as the security team is tracking. This condition is caused by many issues: Shadow IT, adoption of cloud technologies and Software as a Service platforms, legacy systems that have never been tracked, and so on and so forth. One of the first places that good pen testers (and many attackers) start is with open-source intelligence (OSINT), including deep web/dark web research. It's not just credentials and passwords, but systems that are targeted. If a tester can get into a system you aren't even tracking, there is a good chance he/she can gain undetected entry and pivot into more desirable targets. This problem is real enough that Jeremiah Grossman and Robert Hansen, two of the luminaries in the AppSec space, left what they were doing and launched a startup to help companies combat this issue.

The background is a blurred image of a newspaper page. On the left side, there are several columns of text, likely an article or a list. On the right side, there is a large photograph of a woman with dark hair, wearing a dark jacket, looking towards the left. The overall image is out of focus, with the primary focus on the red call-to-action box in the center.

SUBSCRIBE NOW

FOR COMPLETE ISSUE