Building Walls While Leaving the Doors Open
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
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 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.

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
Building a resilient and innovative ASEAN

Our Speakers

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

May-Ann Lim
Managing Director
Asia Cloud Computing Association

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

Mark Johnston
Customer Engineer - Security (JAPAC)
Google Cloud

Vincent Loy
Managing Director
Accenture

Hock Lai Chia
President
Singapore Fintech Association, Singapore

Malikkhan Kotadia
Mentor
The FinLab Pte Ltd, Singapore

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

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

Our Partners

Platinum Partner
DARKTRACE

Gold Partner
Google Cloud

Silver Partner
ivanti

Startup Partner
HORANGI CYBER SECURITY

Supporting Partner
CyberSecurity MALAYSIA

Supporting Associations

Education Partner
EC-COUNCIL UNIVERSITY

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.