CISO MAG
beyond cybersecurity
Volume 5 | Issue 11 | November 2021

IAM Security: Going Beyond the Traditional Security Perimeter

Jeff Barron
Director of Professional Services - Offensive Security
Critical Path Security

58
COVER STORY

ZERO TRUST, IAM & PAM

THE NEW COCKTAIL FOR MITIGATING SECURITY RISKS

CISO MAG

beyond cybersecurity

EDITORIAL ADVISORY BOARD

CISO MAG established an **Editorial Advisory Board** with the foremost innovators and thought leaders in the cybersecurity space. Board members offer the CISO MAG editors advice regarding the magazine as well as suggest the strategic direction it should follow. It includes shaping our editorial content, identifying important topics and special issues, moderating discussions, vetting technical content, and updating the magazine's presence by creating and implementing different initiatives.

The Advisory Board members are "**active**" participants and contribute to CISO MAG regularly. They contribute in either of the following ways:

- Editorial strategy
- Writing articles
- Exclusive quotes for editorial stories
- Vetting surveys and technical content
- Podcasts, webinars, video, and text interviews

Carolyn Crandall

Chief Security Advocate
Attivo Networks

Carolyn Crandall is the Chief Security Advocate at Attivo Networks, the leader in preventing identity privilege escalation and detecting lateral movement attacks. She has worked in high-tech for over 30 years and has been recognized as a top 100 women in cybersecurity, a guest on Fox News, and profiled in the Mercury News. She is an active speaker on security innovation at CISO forums, industry events, and technology education webinars. Carolyn also co-authored the book *Deception-Based Threat Detection: Shifting Power to the Defenders.*

Vandana Verma

Security Relations Leader
Snyk

Vandana is a Security Relations Leader at Snyk with a current focus on DevSecOps. She has extensive experience in Application Security, Vulnerability Management, SOC, Infrastructure Security and Cloud Security. Vandana is a seasoned speaker and trainer. She presented at various public events ranging from Global OWASP AppSec events to BlackHat events, to regional events such as BSides events in India. She is on the OWASP Global Board of directors (Vice-Chair). She also works in various communities towards diversity initiatives such as InfosecGirls, InfosecKids and WoSec. She is a recipient of multiple awards and is listed as one of the top women leaders in technology and cybersecurity in India by Instasafe.

Favour Femi-Oyewole

Global Chief Information Security Officer (CISO)
Access Bank Plc.

Favour Femi-Oyewole has over 23 years of experience managing all aspects of Information Technology with vast knowledge in Enterprise IT Security, Information Technology, IT Governance, Information Security best practices, Cyber Security, Business Continuity, and Risk Management, especially in dynamic, demanding large scale environments. She is also regarded as the first female COBIT 5 Assessor certified in Africa, the first female in Africa to be a Blockchain Certified Professional, and the first woman to win the Global Certified CISO (C|CISO) of the Year 2017. She is a Certified ISO 27001:2013 Lead Implementer Trainer and an Alumni of Harvard Kennedy School (HKS) - Harvard University and Massachusetts Institute of Technology (MIT). She is a member of the Cybercrime Advisory Council in Nigeria with the Mandate of implementing Cybersecurity for all sectors in Nigeria and the pioneer Chair of the Standard and Evaluations Committee. She is a Fellow of the British Computer Society (BCS), The Chartered Institute for IT. She serves as a member of the Global C|CISO Advisory Board and the Information Security woman of the Year 2021 in Nigeria.

Dr. Charlotte M. Farmer

Independent Director

Charlotte is an experienced Director and Board Member with proven value creation across blue chip companies and top-tier general management consulting firms. Over the last 25 years, she has served as Board Chair, Committee Chair, or Board Advisor to 16 non-governmental organization (NGO) boards. Currently, she serves as Board Chair of a tech start-up and advisor to a private equity company in The Carlyle Group portfolio. Her board expertise includes strategy, governance, and turnaround with proven results building high-performing, growth organizations. Her leadership roles in high-tech manufacturing, global operations, finance, and digital transformation would also be an asset to companies eager to expand their footprint or companies in need of turnaround guidance.

Tari Schneider

C|CISO, CRISC, MCRP, ITILF – Cybersecurity Architect, Author & C|CISO Instructor **EC-Council**

Tari Schreider - C|CISO, CRISC, MCRP, ITILf – is a Cybersecurity Architect, Author, Researcher, C|CISO Instructor at EC-Council, and Strategic Advisor at Aite-Novarica Group covering the cybersecurity industry. He is the author of two Amazon top sellers Building an Effective Cybersecurity Program and Cybersecurity Law, Standards and Regulations. He is also a cybersecurity strategist and C|CISO Master Course instructor passionate about making CISOs the smartest people in the room. Tari consults with organizations to guide the transformation of their cybersecurity programs to obtain regulatory compliance and stave off cyberattacks.

Stan Meirzwa

M.S., CISSP, Director
Kean University Center for Cybersecurity

Stanley Mierzwa is the Director of, Center for Cybersecurity at Kean University in the United States. He lectures at Kean University on Cybersecurity Risk Management, Cyber Policy, Digital Crime and Terrorism, and Foundations in Cybersecurity. Stan has over 15 published research publications and is a peer reviewer for the International Journal of Cybersecurity Intelligence and Cybercrime, Online Journal of Public Health Informatics and an Editorial Review Board member for the International Association for Computer Information Systems. He is a Certified Information Systems Security Professional (CISSP) and member of several associations, including the FBI Infragard, IEEE, and (ISC)². He is a board member (Chief Technology Officer) of the global pharmacy education non-profit, Vennue Foundation. Stan holds an MS in Management with a specialization in Information Systems from the New Jersey Institute of Technology and a BS in Electrical Engineering Technology from Fairleigh Dickinson University.

John Kindervag

Senior Vice President Cybersecurity Strategy
ON2IT and ON2IT Global Fellow

John Kindervag joined ON2IT in March of 2021 as Senior Vice President Cybersecurity Strategy and ON2IT Global Fellow. He spent the previous four years at Palo Alto Networks as Field CTO. Before Palo Alto Networks, John spent eight and one-half years at Forrester Research as a Vice President and Principal Analyst on the Security and Risk Team. John is considered one of the world's foremost cybersecurity experts. He is best known for creating the revolutionary Zero Trust Model of Cybersecurity.

Zachery Mitcham

MSA, CCISO, CSIH, VP and Chief Information Security Officer, **SURGE Professional Services-Group**

Zachery S. Mitcham is a 20-year veteran of the United States Army where he retired as a Major. He earned his BBA in Business Administration from Mercer University Eugene W. Stetson School of Business and Economics. He also earned an MSA in Administration from Central Michigan University. Zachery graduated from the United States Army School of Information Technology where he earned a diploma with a concentration in systems automation. He completed a graduate studies professional development program earning a Strategic Management Graduate Certificate at Harvard University extension school. Mr. Mitcham holds several computer security certificates from various institutions of higher education to include Stanford, Villanova, Carnegie-Mellon Universities, and the University of Central Florida. He is certified as a Chief Information Security Officer by the EC-Council and a Certified Computer Security Incident Handler from the Software Engineering Institute at Carnegie Mellon University. Zachery received his Information Systems Security Management credentials as an Information Systems Security Officer from the Department of Defense Intelligence Information Systems Accreditations Course in Kaiserslautern, Germany.

Muhammad Tariq Ahmed Khan

Head of Information Security Audit,
Internal Audit Department, **Riyad Bank, KSA.**

Muhammad Tariq Ahmed Khan is Head of Information Security Audit, Internal Audit Division, Riyad Bank, KSA. He has over 21 years of experience in the Banking industry, in areas such as Information Technology, Cyber & Information Security, Business Continuity Management & Disaster Recovery and related Audits. He has a solid understanding and application of Risk-Based Audit methodology, ISMS (ISO 27001), ISO 22301, NIST and COBIT, IT & Information Security regulatory compliance.

He is a double Graduate (Finance and Computer Science) with one Master's Degree in Computer Science. In addition, he holds a number of professional certifications such as CISA, CISM, CRISC, CDPSE, CISSP, PMP, CEH, ISO 27001 ISMS Lead Implementer & ISO 22301 BCMS.

Tariq has published articles on different topics of Cyber & Information Security and IT Audit and also spoken at regional and international seminars and conferences.

Narendra Sahoo

Founder and Director, **VISTA InfoSec**

Narendra Sahoo (PCI QSA, PCI QPA, PCI SSFA, CISSP, CISA, CRISC and CEH) is the Founder and Director of VISTA InfoSec, a global Information Security Consulting firm, based in the U.S., UK, Singapore & India. Mr. Sahoo holds more than 25 years of experience in the IT Industry, with expertise in CyberSecurity Risk Consulting, Assessment, and Compliance services. VISTA InfoSec specializes in Cyber Security audit, consulting, and certification services which include PCI DSS Compliance & Audit, PCI PIN, PCI SSF, SOC1/2, GDPR Compliance and Audit, HIPAA, CCPA, NESA, MAS-TRM, PDPA, PDPB to name a few. The company has for years (since 2004) worked with organizations across the globe to address the Regulatory and Information Security challenges in their industry. VISTA InfoSec has been instrumental in helping top multinational companies achieve compliance and secure their IT infrastructure.

Sunil Varkey

VP
Forescout

Sunil Varkey has over 26 years of Security leadership experience, with large global corporates in banking, telecoms, ITES, software, and manufacturing. At Forescout he is involved in security strategy, innovation, and stakeholder engagements, prior to this he led Cyber Security Assessment and Testing for HSBC, he also worked with Symantec as CTO and Strategist, Wipro as Global CISO and Fellow, as Head of Security and Privacy at Idea Cellular, and in GE, Barclays and SABB.

AJ Yawn

Founder and CEO
ByteChek

AJ Yawn is a seasoned cloud security professional that possesses over a decade of senior information security experience with extensive experience managing a wide range of cybersecurity compliance assessments (SOC 2, ISO 27001, HIPAA, etc.) for a variety of SaaS, IaaS, and PaaS providers. AJ is a SANS Institute instructor and currently teaches the SEC557: Continuous Automation for Enterprise and Cloud Compliance.

AJ is a Founding Board member of the National Association of Black Compliance and Risk Management professions, regularly speaks on information security podcasts, events, and he contributes blogs and articles to the information security community including publications such as CISOMag, InfosecMag, HackerNoon, and (ISC)².

Dick Wilkinson

Chief Technology Officer
Proof Labs

Dick Wilkinson is the Chief Technology Officer at Proof Labs. He also served as the CTO on staff with the Supreme Court of New Mexico. He is a retired Army Warrant Officer with 20 years of experience in the intelligence and cybersecurity field. He has led diverse technical missions ranging from satellite operations, combat field digital forensics, enterprise cybersecurity as well as cyber research for the Secretary of Defense.

Christina Gagnier

Shareholder
Carlton Fields' Los Angeles office

Christina Gagnier, a shareholder in Carlton Fields' Los Angeles office, is an experienced technology lawyer whose practice focuses on cybersecurity and privacy, blockchain technology, international regulatory affairs, technology transactions, and intellectual property. She advises clients on digital strategy to help them navigate uncharted legal territory, and guides a variety of technology companies and consumer brands through emerging legal and policy issues such as digital currency, the sharing economy, network neutrality, and the ever-changing area of consumer privacy law.

Christina has served on notable committees and task forces, including the Federal Communication Commission's Consumer Advisory Committee and the California attorney general's Cyber Exploitation Task Force. Outside her practice, Christina is an adjunct professor at the University of California, Irvine School of Law, where she serves as clinical faculty for the Intellectual Property, Arts, and Technology Clinic.

EC-Council

Be Unstoppable with
The Ultimate Cybersecurity
Awareness Month Learning Bundle

Get **15 In-Demand Cybersecurity Courses for Just $15**

Start Learning Now

Celebrate Cybersecurity Awareness Month with CodeRed, EC-Council's continuous learning platform!

The Ultimate Cybersecurity Awareness Month Learning Bundle comprises 15 courses co-developed by academia and industry experts. Each course is available to you at just $1. Grab this limited-time offer now!

codered
FROM EC-COUNCIL

The Ultimate Cybersecurity Awareness Month Bundle $15

One Time Payment

- Access to 15 in-demand cybersecurity courses
- Courses co-developed by academia and industry experts
- 1-year access to courses
- Content updates and premium support for 1 year
- Emphasis on 'learning by doing'
- Access available on any device of your choice
- Globally recognized certificate after completing each course

Grab 15 Courses for just $15

Courses in this Learning Bundle:

- Hands-on Android Security
- Black Hat Python: Python for Pentesters
- Identity and Access Management
- Wireless Pentesting with the Raspberry Pi
- Wireshark for Ethical Hacker
- In the Trenches: Security Operations Center
- Hands-on Azure Databricks and Security
- Hands-on Azure Data Factory and Security
- Getting Started with Vulnerability Analysis and Management
- Computer Forensics Best Practices
- End-to-End Mobile Security
- Common Cybersecurity Attacks and Defense Strategies
- Cybercrime and You: Staying Safe in a Hyper-Connected World
- Information Security for Dummies
- Cyberbullying and You: Beating-the-Bully Guidelines

Grab 15 Courses for $1 Each

Start learning with
CodeRed's 'The Ultimate Cybersecurity Awareness Month Bundle' for just $15.

Buy 15 Courses for just $15

Volume 5 | Issue 11
November 2021

Image credits: Shutterstock & Freepik
Illustrations, Survey Design, Cover & Layouts by: Jeevana Rao Jinaga

* Responsible for selection of news under PRB Act. Printed & Published by Brian Pereira, E-Commerce Consultants Pvt. Ltd.,

EDITOR'S NOTE

ZERO TRUST – NO MORE CHEWY CENTERS!

Brian Pereira
Editor-in-Chief

It seems no security conference or conversation is complete without a discussion on zero trust. The zero-trust model and zero-trust architecture are not new concepts, but were devised in the last decade. The terms have increased in popularity since the pandemic struck in 2020, and they are now more relevant than ever, especially as we now find ourselves living in a time in which there is no network perimeter.

The zero-trust model was initially proposed by **John Kindervag** in the fall of 2008. It started with a series of speeches, first at a country club in Montreal, Canada, and continued down the East Coast, ending up in Atlanta, Georgia. Kindervag was then with Forrester Research, and produced a paper that was the result of two years of research. The paper was titled, "No more chewy centers: Introducing The Zero Trust Model of Information Security." Currently, Kindervag serves as the Senior Vice President of Cybersecurity Strategy at ON2IT.

In a recent conversation with *CISO MAG*, Kindervag said there were two worlds back then. The internal network was safe, trusted, and secure. It had the highest level of trust. The external network had the lowest level of trust. He opposed the idea that the network needed to have a crunchy, hardened layer on the outside, and a soft, chewy inside. For a long time, security professionals assumed that malicious individuals wouldn't get past the "hard, crunchy outside," as he writes in his paper. He suggested that there should be a lot of crunchy, and a little bit of softness on the inside, which is the data that needs to be protected. In his words, "Zero trust needs to be like a chocolate chip cookie."

The paper suggested that the way to confront new threats was to eliminate the soft, chewy center and make security ubiquitous throughout the network, not just the perimeter. So, the zero-trust model was created to help security professionals do this effectively.

That definition is more widespread today, with zero-trust architecture extending way beyond the corporate perimeter and onto the cloud and remote access platforms. Trusted identity becomes an important factor here, and is applicable to devices, applications, and people. And that's why identity and access management (IAM) is the new gold standard for information security.

In our cover story on page 58, **Jeff Barron**, Director of Professional Services - Offensive Security, Critical Path Security, writes that IAM augmented with zero-trust architecture and privileged access management (PAM) is what you need to mitigate the risks arising from incorporating emerging technologies. This is the "cocktail" you need to fight modern-day threats.

So, we are way beyond the chocolate chip cookie days.

INDEX

Contents

BUZZ

Zero Trust -
A Security Paradigm Shift

16

OPINION

Stronger Together:
Effective Cyber Defense
Requires the Crisis
Management
and Security Teams to Work
in Concert

24

INSIGHT

Identity Detection and
Response Technology
Gives Zero Trust a Boost

38

PERSPECTIVE

The Missing Piece: Engaging Employees in Building Zero-Trust Environments

46

COVER STORY

IAM Security: Going Beyond the Traditional Security Perimeter

58

KNOWLEDGE HUB

Zero-Trust Architecture Design Principles

70

KICKSTARTER

On a Mission to Make Cyberattacks Irrelevant

80

Zero Trust - A Security Paradigm Shift

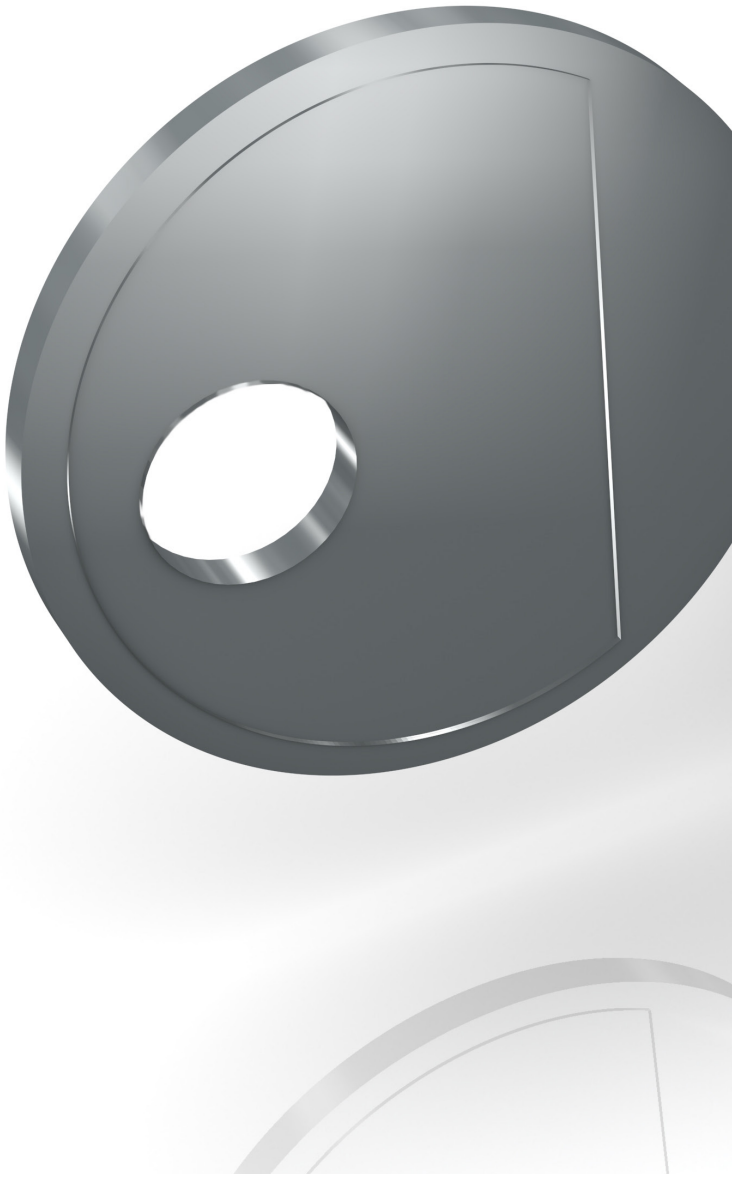
Zachery S. Mitcham
MSA, CCISO, CSIH
VP and Chief Information Security Officer,
SURGE Professional Services-Group

Zero trust is the latest craze in information security circles these days. While not a new concept, its value as a control has come into its own. Cybersecurity compromises (often resulting from common vulnerability exposures) have forced information security professionals to take a more aggressive approach in safeguarding confidentiality, integrity, and availability of enterprise-sensitive data.

Sensitive information is pilfered electronically every single day, all over the world. Zero-trust architecture (ZTA) is a means to reduce the risk of technological systems and data compromise if it is implemented correctly. Organizations must have a continuous diagnostic and mitigation program for ZTA to be successful. End-to-end continuous monitoring of devices that utilize the organization's technological network is essential.

Six elements that make up an Information System. They are hardware, software, networks, procedures, databases, and humans. The weakest link, yet the strongest asset, is the human. As a result, natural tendencies, proclivities, and implicit biases allow for system vulnerabilities. False negatives and positives result as causation of these human frailties. Securing humans begins by educating them on how they are negatively affected by lapses in security.

Cyberattackers often focus on the human as the primary target of their attack. It is therefore imperative that security awareness training is mandated for the workforce throughout the organization. Senior management, from the organization's governing authority to the CEO and all throughout the entire chain of command must set the example by providing leadership and being actively engaged with the effort to maintain a culture of security within the enterprise.




data
security
access
hardware
based
disk
malicious
operating
systems
hacker
protection
encryption
SUBSCRIBE NOW
TO READ THE FULL ISSUE