CYBERSECURITY IS AN IMPORTANT COMPONENT OF DIGITAL TRUST

Daniel Dobrygowski
Head of Governance & Trust, World Economic Forum

UNDER THE SPOTLIGHT

CYBERSECURITY MESH ARCHITECTURE
AN INTUITIVE AND COMPREHENSIVE THREAT MITIGATION STRATEGY
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 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 Schreider
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
Keen 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.
ISOs and security professionals have faced a challenge for years. Much has been said and written about it, but the industry never really got down to solving it. There are a plethora of security solutions serving different functions. But they work independently in silos and rarely “talk” to each other. Each has its own dashboard. So, to get complete visibility into one’s security posture, a CISO must collate information from various dashboards, logs, and reports. The volume and sophistication of attacks have escalated to such a level that it makes this task much more tedious or nearly impossible to do daily. More importantly, the lack of cohesiveness increases organizations’ impact and financial burden. And so, we yearn for that Utopian “single pane of glass” and interoperability between the various security solutions deployed.

According to Gartner, by 2024, organizations adopting a cybersecurity mesh architecture (CSMA) to integrate security tools to work as a collaborative ecosystem will reduce the financial impact of individual security incidents by an average of 90%.

For this month’s cover story, we have Felix Gaehhtgens, VP Analyst at Gartner Inc., explaining CSMA and how it will enable interoperability between the various security tools – to avert or mitigate security attacks. Gaehhtgens offers six actions for security and risk management leaders to enable CSMA.

Gartner has identified Cybersecurity Mesh as one of the top cybersecurity trends for 2022. CSMA provides four foundational layers to enable precise security controls to work together collaboratively and facilitate their configuration and management.

So, will CSMA be effective in mitigating threats? It will take a lot of effort and new strategies to make this work, and the onus is on both, the solutions provider (vendor) and the user organization. It needs to be an industry-wide effort, with vendors coming together to use common architecture to ensure interoperability. We have heard about database connectors, APIs, and other mechanisms that serve as “hooks” to link systems. We need to have something similar for security solutions. Everyone wants to deploy “best of breed” solutions, and one vendor cannot provide it all (though companies like Trend Micro are working in this direction). Unless there is tight integration between the various security solutions and seamless communication between them, we will not have this kind of interoperability.
Contents

CAMPUS CORNER

The Real Value of Professional Certifications
Dr. Charlotte M. Farmer
Independent Director

20

Mastering Art and Science Is Imperative for CISOs to Be Successful
Prasad Jayaraman
Principal, Advisory
KPMG

30

BUZZ

Talking to the Board: How CISOs Can Communicate the Need for Both IT and OT Cybersecurity
Ryan Moody
President & CEO
ABS Group

14
Cybersecurity is an Important Component of Digital Trust

Felix Gaehtgens
VP Analyst
Gartner, Inc.

Cybersecurity Mesh Architecture Can Reduce Financial Impact of Security Incidents

Jeffrey Kok
VP, Solution Engineers, Asia Pacific and Japan
CyberArk

DevOps Engineers are Constantly Being Hunted by Cybercriminals
The Real Value of Professional Certifications

Dr. Charlotte M. Farmer
Independent Director

Whether Lean Six Sigma (LSS), Project Management Professional (PMP®), IT Infrastructure Library (ITIL®), the EC-council’s Certified Chief Information Security Officer (CCISO), or Certified Information Systems Security Professional (CISSP) (the list goes on), the real value of professional certifications comprises multiple perspectives. This brief article highlights the immediate impact, return on investment (ROI), and competitive edge as value-added considerations for seeking professional certifications in cybersecurity.
Rapid Impact

Faced with rapid changes in technology and evolving cyberthreats, leaders quickly find themselves overwhelmed by knowledge and capability gaps. For example, organizations are encountering a significant change in processes and protocols to operate and secure the enterprise effectively. Realizing that the skills needed to execute are becoming radically different, leaders are compelled to reset or upskill the workforce. With the heightened emphasis on mobility, organizations seek application skills that enable the development and management of various cloud services. Organizations and their service providers are upskilling employees through acquisitions, training, retraining, or talent acquisition mechanisms.

Given that certifications deliver targeted guidance in a timely fashion, leaders look to certifications as a rapid approach to keep skills fresh and relevant whenever, wherever needed. Pursuing a degree program is not always a practical option. In some cases (e.g., cybersecurity, AI, data analytics, etc.), textbooks are outdated by the time they are published. Certifications have rapidly become a stop-gap solution to help keep pace with technology acceleration.
Return On Investment

With the rapidly changing demand for new solutions, (e.g., AWS Certified Solutions Architect – Professional, Certified Cloud Security Professional [CCSP], Certified Data Privacy Solutions Engineer [CDPSE], etc.), some organizations may not understand the available capabilities or how to employ them. This cripples leaders as they strive to actualize strategies. Playing the long-game: Once the strategic direction is established, a 2–3-year Information Technology (IT) roadmap should be established to identify:

1. Business needs, challenges, and aspirations.
2. Functional capabilities needed to tackle challenges and achieve aspirational goals.
3. The talent needed to perform capabilities.
4. Professional development needed for the workforce.

In situations where individuals are faced with trade-off decisions between pursuing a certification or degree, it can be helpful to establish criteria that will be used to measure ROI. Criteria could include (but is not limited to):

- Salary impact
- Urgency (needed to address the emerging threat or enable business transformation)