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

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

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

Grab 15 Courses for $1 Each

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!

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

Buy 15 Courses for just $15

CISO MAG
beyond cybersecurity

Volume 5 | Issue 11
November 2021

President & CEO
Jay Bavisi

Editorial

Director, Content & Editorial
Cynthia Constantino*
cynthia.constantino@eccouncil.org

Editor-in-Chief
Brian Pereira*
brian.p@eccouncil.org

Editorial Consultant
Minu Sirsalewala
minu.sirsalewala.ctr@eccouncil.org

Sub Editor
Pooja Tikekar
pooja.v@eccouncil.org

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

Sr. Technical Writer
Dr. Anuradha Nair
anuradha.nair@eccouncil.org

Management

Senior Vice President
Karan Henrik
karan.henrik@eccouncil.org

Director, Digital Marketing
Mayur Prasad
mayur.prasad@eccouncil.org

Senior Director
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

Head - Research & Content
Jyoti Punjabi
jyoti.punjabi@eccouncil.org

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

Asst. Manager Visualizer cum Graphic Designer
Jeevana Rao Jinaga
jeevana.r@eccouncil.org

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

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

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

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.

Gone are the days when baby boomer-era CEOs relegate their IT issues to their organization's experts of the matter with an "out of sight, out of mind" mentality. The U.S. government must impose legislation like SOX during the economic collapse of 2008, when CEOs and CFOs claimed ignorance claimed with respect to having knowledge of what was occurring within their organization's financial operations.

Failure to fully implement zero-trust architecture within the U.S. technological infrastructure grid resulted in the exposure of weaknesses in our Supervisory Control and Data Acquisition (SCADA) systems, thereby placing the SCADA systems at risk of being exploited by future cyberattacks.

Cloud services and technology began to be a game changer in the late 1990s. Today, it is ubiquitous. The scale of these services enables disparate organizations to leverage the computing resources of others thereby making business operations more flexible.

ZTA assists with securing cloud services by diverting primary focus away from the organization's perimeter and shifting more to their resources to outsourced collaborative computing services otherwise known as the cloud. The enterprise can therefore provide security to their data and systems irrespective of where it resides and trusts no user, device, or application until it has been fully vetted via authentication and authorization methods. For ZTA to be effective, it must be embedded

pervasively throughout the enterprise's technological security systems.

U.S. Government Involvement Implications

The U.S. bears responsibility for defending its citizenry, at all levels, against all enemies, foreign and domestic, regardless of the type of attack, cyber, military, pandemic, or directed-energy attacks that are making government employees distressed throughout the world. The response cannot be a decentralized one.

State-sponsored and criminal cyberattackers exposed the U.S. government's lack of preparedness and capability to defend itself against unauthorized information system intruders. Recent SCADA ransomware attacks on our infrastructure; the ransomware attacks on supply chain, and food distribution systems; attacks such as SolarWinds, Colonial Pipeline, and JBS — all sent American citizens into a frenzy, panic, and mass hysteria.

The U.S. government must develop and strengthen international laws with respect to what constitutes a violation of a state's sovereignty relative to cybercriminals and actions that can be executed when such breaches of sovereignty are violated. Additionally, strengthen relationships within the League of Nations to prevent safe harbor of cybercriminals wherever they reside.

Conclusion

What the recent cyberattacks on our country's critical infrastructure have taught us is that we can no longer allow a single attack on a technological system to disrupt the entire eco-system of the U.S.

It's now time for leadership at all levels to re-evaluate their position on what can and cannot operate online. There is a very good reason that we don't vote online in our country and probably never will. Our Department of Defense has two separate networks that they use to conduct secure and nonsecure communications. And, for good reason. I doubt that they would ever think of delivering war plans over the internet. It is a matter of national security and must be seriously considered.

There is no reason why SCADA designed infrastructure and similar technology can't operate effectively off the cyber grid. Prior to online, networked, distributed computing there were no opportunities for our foreign adversaries to attack our infrastructure from remote locations. They were offline. A security paradigm shift is in order.

About the Author

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.

Zachery is also on the *CISO MAG* Editorial Advisory Board.

Disclaimer

Views expressed in this article are personal. The facts, opinions, and language in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.

OPINION

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

Vanessa Vaughn Mathews
Founder and Chief Resilience Officer
Asfalis Advisors

Following a summer of high-profile ransomware attacks, awareness of the danger of cyberattacks is more significant than ever; however, data shows 70 percent of organizations still lack a cyber response plan.

What is behind this shocking lack of readiness? What can be done to improve the situation?

This article will explore possible answers to these questions while also showing that one of the best things an organization can do to jumpstart its cyberdefense program is to create an active partnership between its crisis management (CM), business continuity (BC), physical security, and information security teams.

A Report From the Field

As the founder and chief resilience officer of Asfalis Advisors, I've helped clients in real estate, healthcare, information technology, transportation, logistics, professional services, and government develop, validate, and maintain their business resilience programs. I've also worked closely with corporate security departments to help them mitigate risks, conduct exercises, gain executive sponsorship, and establish the budget necessary to increase resiliency.

These endeavors have given me a front-row seat as organizations have responded — or more commonly missed steps to respond —

to the rising threat of ransomware and data breaches.

This article is a report from the field outlining the challenges and proposed solutions based on what my team at Asfalis and I have seen over the past year or two.

The Importance of a Correct Diagnosis

For any organization that is not prepared for a cyberattack, the first thing to do when developing a cyber response plan is to diagnose the reason for the preparedness failure. What other priorities within the company prevented leadership from investing time and resources in cybersecurity? What's driving this decision?

If you can't see it, you can't solve it.

The failure to plan for a cyberattack is usually a symptom of some other issue. Whether it was a lack of clear guidance or a failure to follow through, organizations need to understand and correct the cause. Focusing on the root problem is the difference between organizations that are sitting ducks and those that are prepared and resilient.

In broad terms, the problem is almost always a failure of leadership.

Drilling deeper, we find that the problem usually arises from one or more of a dozen common shortcomings. Let's take a look at them.

Common Causes of a Failure to Prepare

The following are some of the main reasons that we at Asfalis have identified explaining why organizations have not developed a cyber response plan:

- **Lack of awareness of the risk.** Many employees at all levels are still unaware of the dangers of ransomware and other cyberattacks.
- **A belief that it can't happen to them.** Many executives and staff hold the opinion that even if cyberattacks are a problem for some organizations, such an attack could never happen to them.
- **An inability to articulate the value proposition in being prepared.** Sometimes business continuity and risk management professionals recognize the importance of being prepared but are challenged with explaining what they know to the executives who allocate resources.
- **Staff are unmotivated or bored.** If the people responsible for initiating or implementing positive change are stagnant, change will not happen.
- **Leadership is not approachable.** Sometimes mid-level employees would like to develop a cyber response plan but keep the idea to themselves because senior executives can be known as unwelcoming toward lower-level employees' opinions and initiatives.
- **Executives fear the consequences of speaking out.** Even within the executive ranks, there can be differences of opinion about the value of developing a cyber plan. We've seen executives who are knowledgeable about cyberattacks censor themselves in meetings out of a fear that speaking up about the need to prepare will result in damage to their reputation or career.
- **Failure to invest in the proper infrastructure.** Many companies are still using technology systems from the 1980s and '90s. These might be sufficient to keep the business going under ordinary circumstances, but they are usually not robust enough to withstand attacks by cybercriminals using 21st-century techniques and equipment.
- **Staff lacks sufficient competence and confidence to perceive the threat and execute the needed changes.** It's not necessary for everyone at the organization to appreciate the danger of cyberattacks. However, if no one has the required knowledge and ability, the organization will remain unprepared.
- **Inability to hire the right types of people.** Sometimes, a company wants to hire people capable of creating a cyberdefense program but cannot find them in their geographic area. This can be a real problem for organizations in rural locations.
- **Outdated knowledge and attitudes.** Some companies have long-serving IT teams that are mired in the technology and issues of the past. Such groups can be slow to grasp and respond to today's challenges.
- **Lack of understanding of the threat.** We sometimes see a startling lack of awareness of the most fundamental concepts of modern cyberattacks by high-ranking executives. I've had CEOs tell me their companies don't need to prepare for cyberattacks because they don't store customer credit card data. This shows a lack of awareness of one of the most prevalent forms of contemporary cybercrime, ransomware attacks (where a criminal encrypts a company's data and demands a ransom in exchange for the key). A company doesn't need to store customer credit card data to be a potential target of such an attack. It only needs to depend on computers and data for its critical operations.
- **C-suite staff lack technical expertise.** Except at tech companies, most C-suite executives are usually not technology experts. This can be an obstacle in getting the leadership to grasp the threat of cyberattacks and fund the necessary protections.

- **Inability of technical staff to communicate with business staff.** Often the IT staff are aware of the danger of cyberattacks but are challenged with delivering the message in a manner the business can understand. Since the business staff controls the budget, measures to improve cybersecurity go unfunded.

If you are a leader trying to understand why your organization is not prepared for a cyberattack, the above list is an excellent place to start. Are any of these challenges a factor in your organization?

Achieving Protection Through Partnership

Working with my clients has helped me understand why many organizations fail to prepare for a cyberattack. It has also shown me one of the best things an organization can do to get prepared is develop an active

partnership between crisis management, business continuity, physical security, and information security teams.

In most organizations, the teams handling crisis management and business continuity have little to do with the physical security and information security teams. A lack of collaboration results in a failure of each group to understand how a cyberattack will impact the others and disrupt their ability to carry out critical business processes. This reduces their motivation to work toward a robust cyber defense as a single team.

Having BC and CM teams design schedule cyberattack exercises and invite the physical security and infosec teams to participate has proven incredibly effective at overcoming this problem. Often to the point of motivating the leadership to finally create a cyber response program.

I have been involved in many such exercises as a consultant and facilitator.

I have often watched such exercises, and the conversations that go with them finally make the threat of cyberattacks real to the security teams. The exercises allow the BC and CM teams to show how many hostile actors are trying to break into the network minute by minute and day by day. They also let those teams spell out the impacts that a cyber breach or ransomware attack can have on critical business operations (e.g., "If x happens, you won't be able to bring trucks in here" or "If the hackers do y, we won't be able to answer customer service calls.")

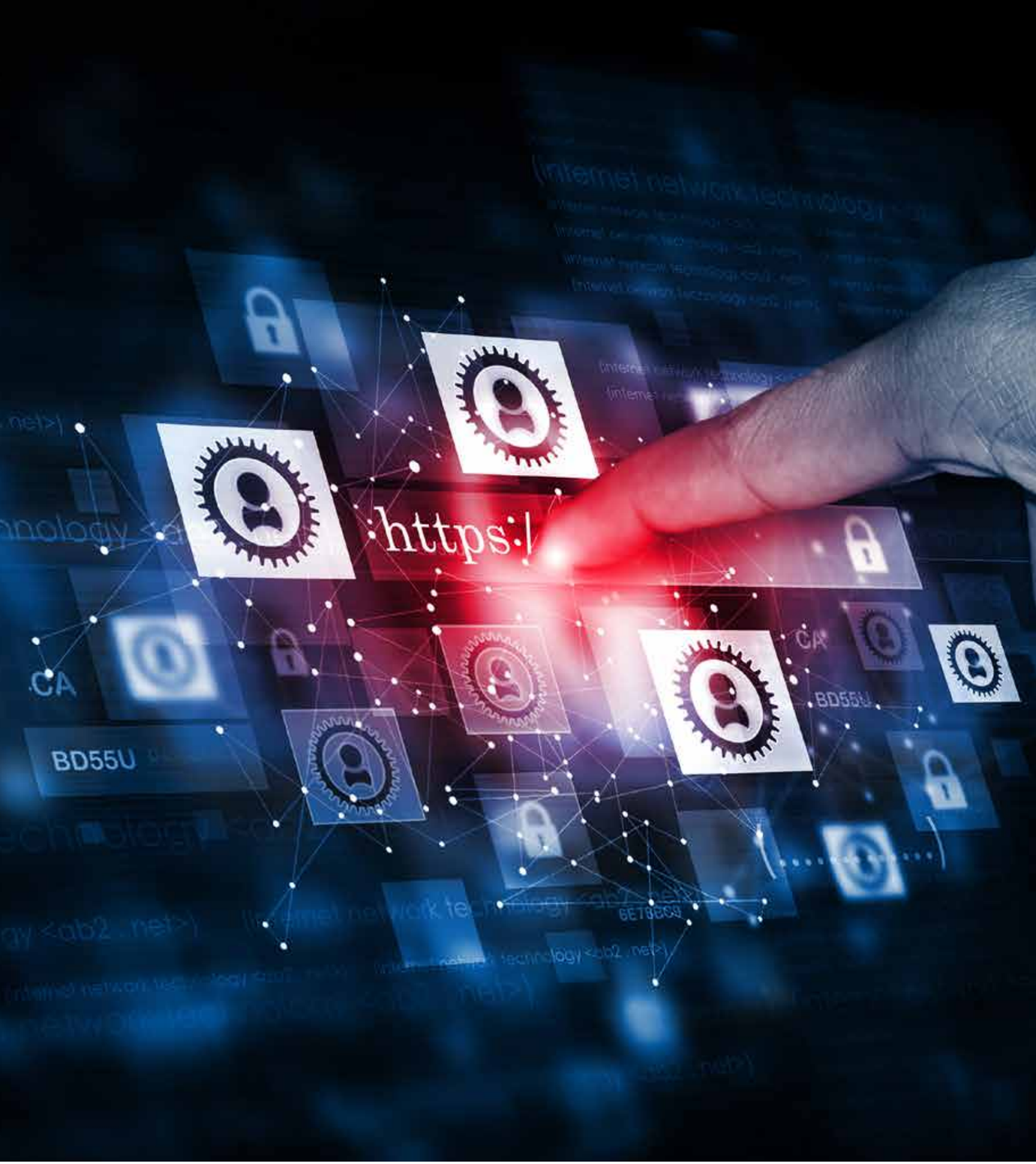
This is often when the light goes on for the physical security and infosec people. These teams commonly go on to become advocates for a stronger cyber defense within the organization.

Their support is valuable for two reasons. One, an effective defense against cyberattacks requires both a business response and a technical response, and the participation of the infosec team is necessary to devise the technical response. Two, the support of the physical and infosec teams, added to that of the CM and BC teams, is often enough to tip the balance in getting the leadership to take cybersecurity seriously and fund the necessary defensive measures.

These four teams truly are stronger together. By working in partnership, they can often win the support of their leadership, bringing about needed change and helping their organizations go from being potential helpless victims of cyberattacks to being strong, prepared, and resilient.

Creating a Constituency for Change

Unfortunately — and shockingly — only 30 percent of organizations currently have a cyber response program in place. The first step for any organization that wants to improve its cybersecurity is to identify why it



has neglected to do so so far. The broader cause usually stems from leadership. The specific causes can include anything from lack of awareness of the threat on the part of the executive leadership to the inability to hire cyber-savvy staff due to geographic isolation.

One of the best ways for an organization to jumpstart its cyberdefense program is for the CM and BC teams to invite the physical security and information security teams to join it in a cyber incident exercise. This often makes the risk and potential impact of a cyberattack real to those teams for the first time. This can create a broad constituency for change within the organization, a constituency that just might be strong enough to move the senior leadership to finally make the investments necessary to protect the organization against cyberattacks.

About the Author

Vanessa Vaughn Mathews has been on the front lines of the crisis management and business resilience profession throughout her career. She is the first female in the state of Georgia to graduate with a degree in Homeland Security and Emergency Management. She has worked with a Tier 1 intelligence agency, *Fortune 500* companies, and has received local, national, and international recognition for her work to restore business and community resilience. She is a sought-after speaker for conferences and professional events as well as civic and private sector initiatives.

Identity Detection and Response Technology Gives Zero Trust a Boost

Carolyn Crandall
Chief Security Advocate
Attivo Networks

Zero trust has been a hot topic in the cybersecurity community for several years, mainly because attackers have gotten better at bypassing perimeter defenses and infiltrating networks. All too often, they are free to move laterally with little fear of detection once inside. Zero-trust architecture (ZTA) provides an added layer of in-network security by treating all identities as potential threats and preventing access to data and resources until it authenticates and authorizes the user.

Unfortunately, ZTA isn't a single, easy-to-obtain product or service. It's an ideal that organizations should strive for, but it is ultimately more of a journey than a destination. And as cybercriminals shift their approach toward identity-based attacks, Identity Detection and Response (IDR) technology has emerged as an essential way to fill in the ZTA gaps left by other in-network defenses.

Identity Exploitation Remains Rampant

Zero-trust architecture combines multiple security approaches, including identity management, asset management, application authentication, network segmentation, and threat intelligence. It is important to remember that treating all identities as potential threats doesn't just apply to user identities. User trust is just one element of ZTA, alongside device trust, transport/session trust, application trust, and data trust. To be effective, ZTA must consider more than just

whether an individual user is authorized. It also needs to consider the device or application used to access the network, the data accessed, and other factors.

Part of the reason for the rush to adopt ZTA is that cybercriminals have gotten very good at exploiting these various identities. The 2021 Verizon Data Breach Investigations Report indicates that credential data now factor into 61% of all breaches, while Gartner also estimates that "75% of security failures will result from inadequate management of identities, access, and privileges" by 2023 — up from 50% in 2020. These statistics shouldn't come as a surprise, given that many network defenses do not detect suspicious activity from what they perceive to be valid identities. A cybercriminal with a set of stolen credentials can often use it to access the network and move laterally throughout it undetected, naturally making credential theft and other identity-based attack techniques extremely popular among adversaries while further highlighting the need for ZTA.

Privileges and entitlements also factor heavily into a comprehensive ZTA approach. ZTA should operate on the principle of least privilege: an identity should only have the right to access data or areas of the network it needs to fulfill its job or function. This limited set of privileges helps ensure that even if an attacker can compromise an identity, that attacker cannot access anything outside that identity's usual purview. For this to work, organizations must thoroughly understand the rights and privileges of each identity present in the network, but many lack this level of visibility.

Filling in ZTA's Identity Security Gaps

Identity Detection and Response or IDR is a relatively new category that arose to address certain gaps in identity protection — and thus broader zero-trust architecture. IDR detects credential theft, privilege misuse, and risk entitlements that create attack paths to high-value targets like Active Directory (AD).

Existing identity tools and categories like Identity and Access Management (IAM), Privileged Access Management (PAM), and Identity Governance and Administration (IGA) tend to focus more directly on authorization and authentication. IDR tools (or solutions) don't just ensure the right identities have access to the right information — they provide greater visibility in entitlement exposures, credential misuse, and privilege escalation activity. These capabilities are especially valuable as organizations continue to migrate to the cloud, since IDR protections extend from the endpoint into multi-cloud environments. And with the number of cloud-based identities continuing to skyrocket, the ability to extend this critical element of ZTA into cloud environments is essential.

IDR is a foundational step in the right direction. IDR solutions actively look for attacks targeting identities rather than collecting data for later analysis like Endpoint Detection and Response (EDR) and similar solutions. The "active" nature of this defense

is significant. When an IDR solution detects attack activities, it feeds fake data back to the attacker, redirecting their attack away from valuable assets and toward decoys. Most IDR solutions can also isolate a system believed to be compromised, keeping the attacker walled off from the rest of the network.

IDR's role alongside identity exposure visibility is also important to note. As the saying goes, you don't know what you don't know. You also can't protect what you don't know about, and too many organizations lack visibility into exposed credentials, overly permissive entitlements, AD (Active Directory) misconfigurations, and other vulnerabilities. Identifying and remediating these issues can significantly shrink the attack surface, leaving attackers little room to operate. Together, IDR and identity visibility tools present a powerful package in avoiding, stopping, and derailing threats.

Embracing IDR to Improve ZTA

It is easy to draw a straight line from IDR to ZTA. By introducing an active defense element to identity protection, IDR adds a new layer of security on top of today's existing tools. Zero trust isn't a single product — it's a category of defense technologies that embrace the principles of ZTA to address the vulnerabilities that today's attackers are continuing to exploit. And with identity-based attacks making up a significant percentage of today's threat landscape, embracing IDR as a way to shore up the gaps in your Zero-trust architecture isn't just smart — it's essential.

> IDR and identity visibility tools present a powerful package in avoiding, stopping, and derailing threats.

About the Author

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*.

Carolyn is on the *CISO MAG* Editorial Advisory Board.

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

Christina Gagnier
Shareholder in Carlton Fields' Los Angeles office

With the recent proliferation of "zero-trust" environments in enterprise security, there has been an implementation bias toward technological solutions to secure data and prevent unauthorized access to systems. When the approach is driven by IT and other technical teams inside an enterprise, it should be no surprise that this would be the case. This is not a criticism but rather a reflection of domain expertise. Businesses should rely on their resident experts to implement the technical infrastructure necessary to protect business assets and personal data.

Due to the fact that employees and teams have been working in a distributed fashion throughout the COVID-19 pandemic, employing technological solutions that can be remotely deployed is also an efficient means to arrive at a zero-trust security environment.

As a result of the new work-from-home paradigm, many businesses rushed toward multifactor authentication and other forms of identity access management. Yet, the state of enterprise security is still, in large part, subject to human error. Once employees verify their legitimate access to business systems, they begin to operate from the knowledge basis of how they were trained and supported to understand security risks.

In moving toward zero-trust environments, businesses must turn their focus to "security by design" principles and, specifically, by revisiting the oft-forgotten principle of "psychological acceptability." This principle, at its core, focuses on (1) the avoidance of security measures being seen as obstructions to users which they are intent to work around and (2) methods to encourage or invite users to embrace given security measures.

Zero Trust Still Needs a Human Touch

The missing piece in most enterprise security programs is the support of employees and real training. To assume that mandatory security training is going to cut it for most employees is a dangerous assumption.

It is not about training the right team. It is not even about training members of all teams on how to identify security threats.

Employees must be meaningfully engaged in the protection of business assets and systems and understand this to be a part of their job functions. Information made available to employees, their training, and ongoing support must be tailored to specific roles and job functions.

Policies must be developed in a manner that appreciates the existing roles and responsibilities of each employee. When a training or tabletop security exercise is added to existing job functions, it is viewed as an extra burden. When training and support are built into job roles and functions, it is clear to employees that security, and ethics in data management and governance, are part of the corporate ethos. The business is demonstrating a commitment to its security practices.

Communication is an important part of implementing meaningful security measures. Different employees come to the table with different skill sets and experience with privacy and security. If it is not communicated to employees how security measures apply to them and their distinct job roles, it's as if two individuals are talking past one another. The teams responsible for security are speaking a technical language and advocating for the architecture and solutions that they had the decision-making authority to choose; the other employees are forced to accept this architecture and solutions without a true understanding of why they are important.

Employees have to be empowered to report security risks. Technological solutions cannot be communicated to employees as the be-all, end-all. For example, if the implementation of multifactor authentication is the direct result of an unauthorized access incident, and it is communicated that the multifactor authentication is the solution to the problem, this approach may overlook the "human mistake" factors that could still lead to future incidents involving unauthorized access or other security breaches. These technological solutions do not necessarily address the litany of other ways businesses find themselves facing a security breach.

People and systems, not just systems, are ultimately responsible for successful security programs.

Zero Trust Should Not Erode Trust with Employees

Beyond some of the obvious technology implementations that allow businesses to verify the identities of the individuals

logging into their systems, many companies have implemented various forms of remote monitoring technologies to monitor employees' work and performance throughout the day. While the prevalence of these technologies may be suited better to some industries than to others, they must be implemented with care and respect to U.S. state laws and the laws of other jurisdictions in which a business may operate. Businesses should ensure that they have a legitimate, legal basis for implementation. A business should be ready to engage in an open dialogue with its employees, about why the implementation is necessary. Further, in some U.S. states and other jurisdictions, consent must be obtained for the implementation of such monitoring technologies.

Business decisions around security must factor in the principle of psychological acceptability. These technologies should also be evaluated for their reception in your particular business environment as that will lead to whether such technologies will be efficacious. If employees are made to believe they are part of the problem (i.e., they did something wrong that has led to the implementation of these technologies and that their personal autonomy and space is being intruded upon as a result), they are less likely to be engaged in the security of the company and the data of which the company is a steward.

The "Why" for Enterprise Security

The larger question regarding truly institutionalizing an ethos with employees around security is determining the driving force behind security programs. The unfortunate reality is that many businesses continue to place policy and technical Band-Aids on security problems rather than approaching security from a "security by design" perspective. Security is not infused into every company process. Rather, it is applied on an ad hoc basis when deemed necessary, which is often driven by an outside force. The rapid acceleration of zero trust throughout the COVID-19 pandemic was driven by the pandemic and the need to quickly get organizations of all sizes operating remotely, at as close to the same capacity as they were operating pre-pandemic. It is hard to know if this acceleration would have occurred without the necessity for it.

There are other "why" factors for the implementation of security measures, and businesses should take care to evaluate whether the right factors are the ones propelling the development of their security policies, programs, and systems.

Customer Demands

If customers (not users) are driving the need for enhanced enterprise security measures, through contractual demands placed on a business or organization to assist in business development and customer acquisition, these measures may be specific to the customer versus purposefully being built

Disclaimer

Views expressed in this article are personal. The facts, opinions, and language in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.

into the policies, programs, and systems of the business. Having different customers with different rules of the road for each use case results in a patchwork of security approaches that effectively become a customer appeasement strategy versus a comprehensive security program.

Regulation

If regulation serves as the driving force behind the implementation of new security measures, there is a tendency for businesses to see the regulations as a "floor" instead of reaching for the "ceiling." Many businesses evaluate regulations for what is precisely required to comply with a specific regulation. When the implementation of enterprise security measures flows from an obligation versus an aspiration to protect the business's customers and employees, the security program will likely miss the mark.

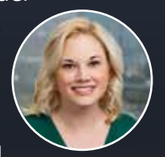
Users and Data Stewardship

If protecting users and data stewardship is the driving force for adopting "best of breed" security, this requires an intentional design of privacy and security programs in such a manner that privacy and security are embedded in every policy, program, and system of the business. This is a much more involved approach but, in the long term, is the approach most likely to avoid costly security issues that may emerge.

Balancing the Elimination of User Error and User Buy-In

Zero trust is about eliminating user error. The benefits of this elimination of opportunity for users in systems to cause massive exposure to a business are clear; but regardless of the technology advancements, businesses are still driven by the people who manage them and work for them. The absence of supports for employees in this new paradigm may create scenarios in which reliance on systems that seemingly eliminate the need for voluntary employee security measures may, as an unintended consequence, create new security risks.

About the Author



Christina Gagnier, 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 has served on notable committees and task forces, including the Federal Communications Commission's Consumer Advisory Committee and the California attorney general's Cyber Exploitation Task Force.

Christina is on the *CISO MAG* Editorial Advisory Board.

IAM Security: Going Beyond the Traditional Security Perimeter

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

The identity and access management (IAM) framework is the new norm of information security recommended as a mandate by cybersecurity experts across various industries. The pandemic enabled remote working, and the recent surge in cybersecurity incidents has made the susceptibility of the new perimeter to threats evident. Even federal government and national agencies have been pressing organizations hard to adopt the access management and zero-trust model to secure their information security architecture.

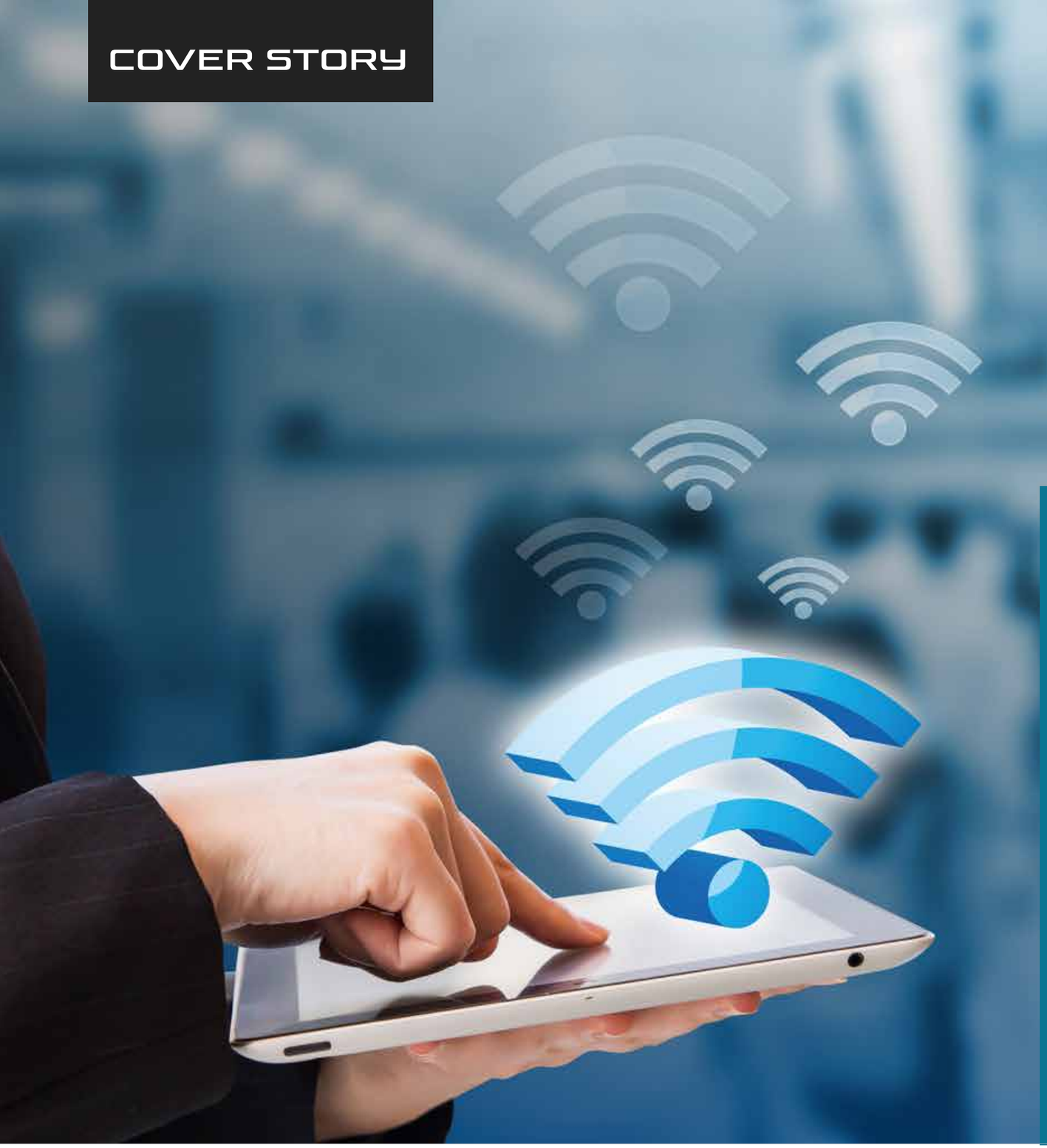
Identity and Access Management to Address Critical Data Risk

The IAM framework aims to define the process, policies, and technology to manage and monitor digital assets and identities that try to access the organization's crucial information. Information technology and security stakeholders of an organization could control the user access to data with the help of access management. The IAM framework involves the use of methods and technologies such as user identity management, user provisioning, multifactor authentication, privileged access management, user authorization, and activity/anomaly reporting. These elements provide the security team with the ability to securely store and manage identity and profile data, such that only the relevant data is provided to the authorized seeker.

Data governance through IAM could be deployed on both, on-premises and virtual cloud environments, or even in a hybrid architecture. Technological concepts of access management could simply be understood as the process of how individuals and their roles are identified by the network and how the network assigns these roles. For a seamless integration and operation of this technology, it is important for the availability of a process to add, remove, or update user roles in the system while protecting sensitive data.

Access Management in Recent Times

The global pandemic has adversely impacted information security. With the abrupt shift to remote working practices, the route of access to sensitive data shifted outside the organization's security perimeter through a public/unsecured network. While immediate measures employed virtual private networks (VPN), many organizations understand the need for securing their data while simultaneously making it available for remote work at all hours. This led to a rapid increase in the adoption of cloud computing and storage services or reconfiguring the networks to satisfy the requirements of remote workforces. Many believe that this transformation has to some extent, mitigated the traditional threats but also introduced more attack surfaces associated with the incorporated technology. The ease of deploying cloud computing tools and services could also make its management difficult for the security team.



The thing to remember about IAM is that we've been working on this problem for a long time. The old-fashioned techniques of phishing, credential stuffing, and password spraying will continue to be used to bypass these security controls.

The thing to remember about IAM is that we've been working on this problem for a long time. The old-fashioned techniques of phishing, credential stuffing, and password spraying will continue to be used to bypass these security controls.

The cloud and work from home security conundrum have made it evident that any slight change in the existing security posture will yield multiple attack surfaces to the threat actor. This calls for specific provisions, policies, and technology to be in place to protect networks, devices, apps, and data before the transformation. To mitigate the risk arising from incorporating emerging technologies, IAM is augmented with zero trust architecture and privileged access management (PAM) concepts.

Going Beyond Traditional "Border & Fence" Security with Zero Trust

The zero-trust architecture enables robust information security for an organization's network by assuming zero trust, i.e., no user or entity is trusted and needs stringent verification. The traditional security operations relied on one-time network perimeter validation and unrestricted access to those inside the perimeter. But, the cloud technology, virtualizations of digital assets, and access to data over the public network have provided the opportunity for the threat landscape to evolve, rendering these measures insufficient.

With zero-trust network access proving to be a means to increase the security provided by the access management framework, more and more organizations are beginning to plan zero trust policy implementation. Zero trust is no longer optional but a mandatory strategy for securing information assets. The areas that are most impacted in security posture due to Zero Trust Network Access (ZTNA) are identity and access management, followed by web security and network security.

Zero-trust solutions could be implemented seamlessly provided the IT architectures are managed properly without further burdening the security team. This calls for trusted managed security service providers (MSSP) or cloud service providers (CSPs) to bear the security workload. ZTNA combined with MSS and cloud service is an effective strategy for organizations to take control of their networks, applications, technology, and data security.

Security Attributes of ZTNA

The ZTNA strategy involves technologies such as multifactor authentication and network micro-segmentation to restrict access of data to unauthorized users to the maximum possible extent. Network segmentation assigns devices and digital assets to their respective network zones based on their feature, function, and purpose within the network. The "least access policy" approach guarantees that users are granted minimal access to networks or data according to their roles and identity. Zero-trust models go beyond one-time validations and mandate the organizations to establish proper security controls to vet every request to engage applications, assets, or access data. This is particularly helpful in the ecosystem where threat and user identity change frequently or fluctuate in volume.

Zero-trust models provide real-time visibility into information such as access points, firmware, number of privileged devices, device geolocation, endpoint applications, incident response protocols, user identification, authentication data, etc. The zero trust model assumes the network to be already compromised, hence disregarding the previous user network behavioral history. Due to its concept of least privilege, every request, user, or connected device is assigned zero trust and needs to be evaluated continually on a per transaction basis. The ZTNA framework could be tailored according to the requirement of the businesses and compliance. This helps every industry with varied information technology postures such as remote working, cloud storage and service, mobile applications, and third-party service involved with the business process.

Managing Privileged Access for Security Resilience

Though zero trust teaches "trust no one, test everyone," not every identity is limited to regular roles. There also exists users,

accounts, processes, and systems with elevated access and permissions across the IT environment. The role of the privilege access management (PAM) strategy is to exert control over such privileged accounts and users, which will help the organizations reduce its attack surface and mitigate vulnerabilities arising from both external attacks and insider threat or negligence. At the core, both PAM and ZTN aim to enforce the principle of least privilege and are defined as access restrictions and permissions for users, accounts, applications, systems, devices, and requests. Managing the privileged access level through PAM or privileged identity management (PIM) is an important security project for reducing cyber risk.

Though necessary, these privileges are accompanied by various risks such as lack of visibility or awareness, over-provisioning, and insider threat. Unmanaged and forgotten privilege account or credentials or over-provisioning due to fear of hindering productivity are some of the prime causes for misuse or privilege-based threats. Many IT operations are distributed and need continuous access, leading to shared accounts or credentials, which may create security, audit, and compliance-related issues.

PAM to Augment Zero Trust

Zero-trust architecture framework is more of a guide than technology that tries and limits user access and works under the assumption that the network is already compromised.

Privilege access management furthers on this to scrutinize privileged accounts and credentials to mitigate insider and external threats. Organizations need to consider a risk-based approach for implementing ZTNA and PAM to avoid vulnerabilities such as default credentials and built-in privileges to achieve control over identity security.

With the incorporation of cloud technology, privileged access management must be scalable to the cloud. There exists a need for context-based privileges, user verification, and continuous authentication to secure modern privileges from misuse. Some utilities in the public cloud lack PAM and need to be addressed from enterprise-level users' compliance and business requirement for both remote and core privileged access. Another simple strategy that could be leveraged by the PAM and ZTNA is to implement least privilege controls on endpoint devices. This involves restricting local admin privilege and other elevated permissions, which in case of need are granted through a stringent and monitored access approval process. Similarly, managing business-critical systems, applications, and data access control, is also a part of PAM strategies.

Accounts that have access to business-critical systems and applications are termed high-risk accounts as these systems govern crucial business operations. Hence, PAM strategies also involve monitoring such an account and its behavior along with security methods such as encrypting credentials, multifactor authentication, credential rotation/change, and restricted session and access location. It is crucial for PAM to strictly control the process that defines or governs privilege assignment and creation, as threat actors aim at creating new privileged accounts or escalate privilege for lateral movement.

Conclusion

Identity and access management can mitigate and reduce a large section of threats associated with unmanaged user identities and access to organizations' sensitive data. Towards these efforts implementing the zero-trust network is the need of the hour, especially when the pandemic has pushed the traditional security and IT architecture onto the cloud and remote access platforms that present a whole new attack surface for the cybercriminals to exploit. Zero trust is all about ensuring appropriate access to critical assets, which is further augmented by monitoring the privileged account and credentials through privilege access management. Organizations initiate the zero trust security journey by prioritizing high-risk assets and using ZTNA as a baseline to build trust scores that can be used to determine the appropriate level of security. With new technologies making their way into businesses across different industries, a need to move beyond zero trust to adaptive risk-based security could be seen. Integrating a privilege management approach for protecting endpoints, applications, and workloads is also a viable option in the near future, but above all, there is a pressing need to create awareness about the importance of cybersecurity with a guide to safer and secure online operations and data access.

> Some utilities in the public cloud lack PAM and need to be addressed from enterprise-level users' compliance and business requirement for both remote and core privileged access.

About the Author

Jeff Barron works as the Director of Professional Services - Offensive Security for Critical Path Security. He has extensive experience with penetration testing, information security, and software development. Jeff is also an active speaker and has been interviewed as an expert on 11Alive NBC News.

Disclaimer

Views expressed in this article are personal. The facts, opinions, and language in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.

Zero-Trust Architecture Design Principles

Tari Schreider
CICISO, CRISC, MCRP, ITILf – Cybersecurity Architect
Author & CICISO Instructor EC-Council

KNOWLEDGE HUB

Zero-Trust Architecture (ZTA) is a design concept, first envisioned by the former security practitioners consortium known as the *Jericho Forum* in 2004. The working premise, put forward by David Lacey, was the perimeter is indefensible. Forum members universally believed traditional network and system security architecture and design approaches could not protect the day's businesses properly. Security architects required a paradigm shift in thinking on how data should be protected. This shift in thinking was referred to as de-perimeterization, which was first described by Jon Measham, a former Royal Mail employee, in a 2001 research paper. Attempting to confine data behind a corporate firewall, restricting it to a controlled network was one of the biggest contributing factors to poor security architecture designs over the last nearly two decades. It inhibited the monetization of data placing a drag on innovation and growth. The Open Group now holds the compass to the zero trust movement. Credit, where credit is due, belongs to the *Jericho Forum Commandments* that formed today's zero trust vision. The adoption of zero trust has been slow but is gaining momentum. What once was old is now new again.

The zero-trust movement has had a meteoric rise since the onset of the COVID-19 pandemic. The lean-in workplace quickly became the get-out workplace, scattering users and data to the four corners of the world. Organizations had to accept a hybrid workforce, with many employees working

from home, and devise new ways to protect data. The cybersecurity industrial complex swooped in to offer all manner of security salvation in what one could refer to as "zero trust washing." Suddenly every product is the silver bullet to deploying a zero-trust model. In April 2021, Microsoft published the results of a global research study of 900 senior security decision-makers around the adoption of a zero trust strategy. 96% of the participants stated that zero trust is their number one priority. Zero trust is here to stay; CISOs should prioritize this but ensure proper design and architecture are applied to avoid piecemeal adoption.

There is no better way to design and architect anything than by referencing an authoritative standard or framework. This standard is the National Institute of Standards and Technology Guide on Zero Trust Architecture–Special Publication (NIST SP) 800-207. Published in August 2020, this standard provides an abstraction definition of ZTA, providing deployment models and use cases where zero trust could improve an enterprise's information security posture.

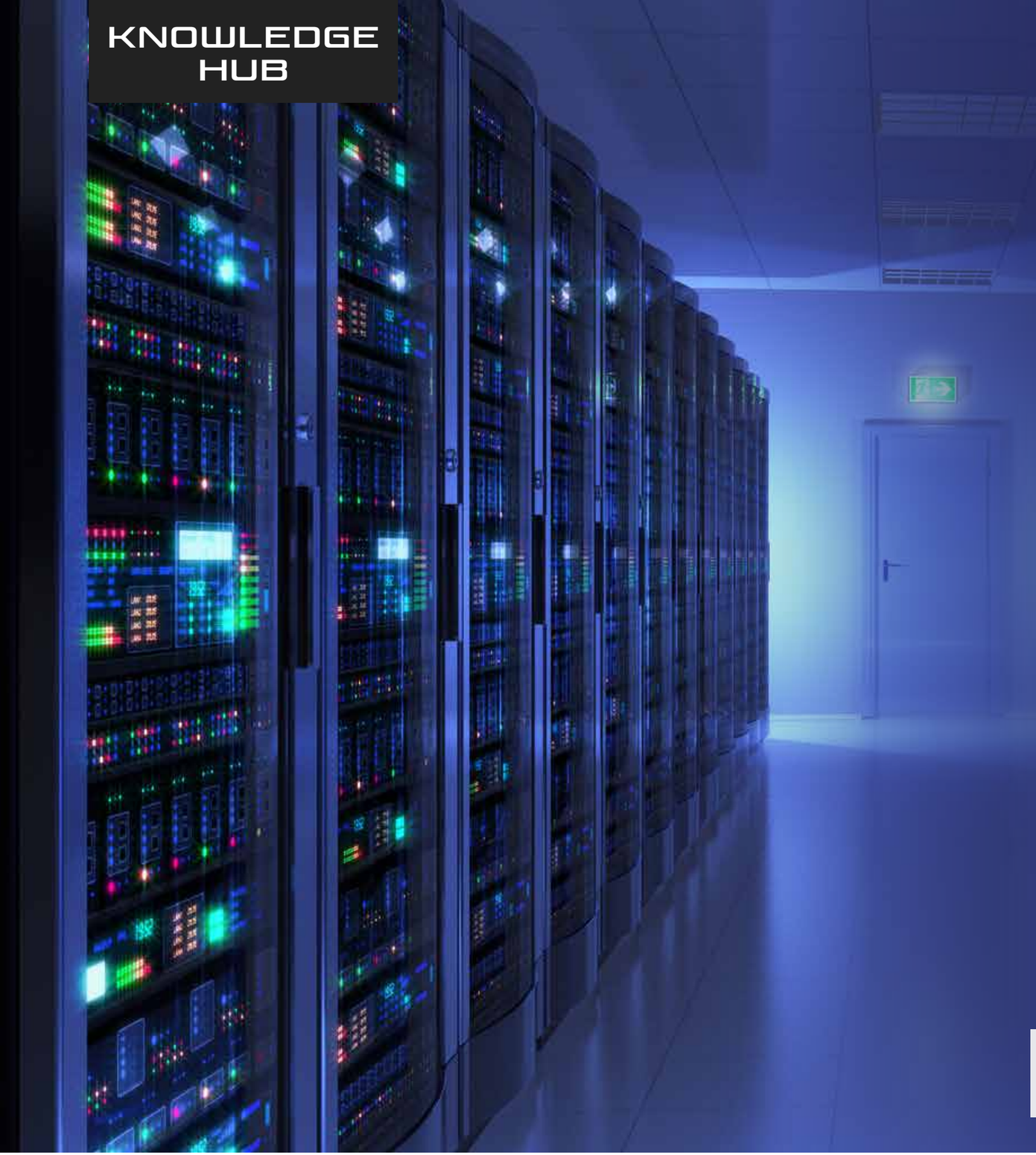
NIST SP 800-207 goes beyond the early definition of zero trust as primarily an access and connection authentication and authorization management approach. Its nearly sixty pages are chock-full of architectural guidance CISOs, and security architects should consider. CISOs can reference the NIST standards prescribed tenants of a zero-trust model compared to efforts underway or completed in deploying their organizations. It is important to remember that ZTA should not be deployed in isolation but integrated with a comprehensive security program.

Zero Trust Design Principles

The diversity and complexity of an IT estate have allowed organizations to deploy zero trust at singular points, often without the benefit of an overall design or roadmap. This approach led to incomplete and ineffectual zero trust deployments. Controlled data and asset access and use regardless of location (e.g., cloud, on-premises) is at the core of architectural design requirements. One fundamental belief of adopting zero trust, without which there can be no zero trust, is that attackers are already present in the IT estate, and the estate is no longer trustworthy. Once that truth is accepted, the work of designing a zero-trust architecture can commence. The following table shows the seven principles of zero trust curated from NIST SP 800-207.

ZERO TRUST DESIGN PRINCIPLES

No.	Zero Trust Principles	Analysis
1	All data sources and computing services are considered resources (physical or virtual components with limited availability).	Data and assets should be classified by criticality, including bring your own devices (BYOD), cloud computing, and third parties. A full discovery of an attack surface is necessary.
2	All communication is secured regardless of network location.	No network connection implies trust. Access requests from any source should meet the same criteria of least privilege and need to know principles. Communications should pass the litmus test of the CIA Triad of confidentiality, integrity, and availability.
3	Access to individual enterprise resources is granted on a per-session basis.	Each session request should be challenged based on assuming an attacker is the one attempting access. Authentication and authorization protocols should not be inherited between resources or sessions.
4	Access to resources is determined by dynamic policy — including the observable state of client identity, application/service, and the requesting asset — and may include other behavioral and environmental attributes.	Users of resources should have a strong unimpeachable identity. The finest grain access control should be deployed where extensive user and object attributes are matched to grant access.
5	The IT enterprise is chartered with monitoring and measuring the integrity and security posture of all owned and associated assets.	No, IT estate assets are trusted, their security posture is continually monitored and evaluated. Assets should always reflect the highest discipline of hygiene. Assets with an unknown state should never be allowed access to the enterprise.
6	All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	Access authentication and authorization are continuous, never ceasing, always assuming that users and assets are untrusted. Identity, credential, access management (ICAM), and asset management should be deployed and integrated to enforce access requests strictly.
7	The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.	Comprehensive vulnerability scanning, threat monitoring, and asset discovery should be performed to assess the IT estate's security posture continually. Analysis should drive revisions to zero trust policies and practices.



> Avoid the temptation of acquiring zero trust products and cloud-based services before designing an architecture.

Summary

Zero trust is not a singular technology, but an end-to-end architecture comprised of policies, procedures, processes, practices, and a technology stack designed to prevent east-west malicious movement. Avoid the temptation of acquiring zero trust products and cloud-based services before designing an architecture. Remember the basic blocking and tackling of understanding data flow and exchange as a precursor to designing a zero-trust architecture. Follow an authoritative zero trust design standard such as NIST SP 800-207. Seek further implementation guidance from companion standards such as NIST Cybersecurity Framework and NIST SP 800-53 Rev. 5. Remember that deploying a ZTA is not intended as the architecture for an entire information security program but simply one integrated schema of the overall information security program.

About the Author

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.

Tari is on the *CISO MAG* Editorial Advisory Board.

Virsec: On a Mission to Make Cyberattacks Irrelevant

Minu Sirsalewala
Editorial Consultant
CISO MAG

KICKSTARTER

Startups are like rulers of small territories at battlefields; ambitious plans to conquer and change the world but with limited arms and resources. Does luck favor them?

Disruptive technology and innovation feed the security industry. In the past, there was a preconceived notion that only the network was under attack. Today, it is increasingly understood that the application is the "asset," and it is also under attack and needs protection. Security needs to go where the application workload goes. And thus Virsec, short for Virtualized Security, came into being.

Virsec creates a dynamic golden image of what your software is supposed to do — and immediately stops anything that it's not. Its mission is to make cyberattacks irrelevant by fully protecting software while it is running in real-time.

Given the precariousness of the situation, cybersecurity has become a national priority. Most recently, even the White House, which has been reiterating the importance of cybersecurity, called upon tech companies such as Google, Microsoft, Apple, and IBM to discuss cybersecurity initiatives to thwart cyberattacks across the U.S.

The brainchild of Satya Gupta, co-founder and CTO, Virsec was founded with the audacious goal of 'ending hacking,' as Gupta believed he had a solution. As Gupta likes to articulate, "While software is 'eating the world', we will stop hackers from 'eating' the software."

He believes success comes by seeking to achieve a large dream or vision and coupling this drive with humbleness, tremendous curiosity, and a thirst to learn from the customers.

> While software is 'eating the world', we will stop hackers from 'eating' the software. We envision a fully safe digital ecosystem that enriches the lives of all countries, companies and citizens.

FOUNDING TEAM

Dave Furneaux
Co-founder & CEO
Virsec

Dave Furneaux has been a driving force behind Virsec since its inception, as an investor and active board member, becoming CEO in 2020. In his career spanning three decades Furneaux has been an entrepreneur and venture investor, forming, building, and investing in numerous high growth companies in information technology, including successful cybersecurity companies, Watchfire (acquired by IBM), Skystone (acquired by Cisco), Application Security (acquired by Symantec) and Aironet (acquired by Cisco). As an early-stage investor in Virsec, Furneaux has played a critical role in guiding its strategy and growth. He holds a BA with Phi Beta Kappa, Magna Cum Laude honors from Colorado College.

Satya Gupta
Co-founder & CTO
Virsec

Satya Gupta is Virsec's visionary founder, with over 25 years of expertise in embedded systems, network security and systems architecture. Gupta has helped build and guide the company through key growth phases from initial funding (2015), developing core technology with key partners including Raytheon and Lockheed (2016-2018), to launching an enterprise-class GA product (2019). Prior to this, he built a highly profitable software design and consulting business targeting data networking, application security and industrial automation projects. He was also Director of Firmware Engineering at Narad Networks and Managing Director and Chief Engineer at Eastern Telecom and Tech Ltd. Gupta has more than 20 patents in complex firmware architecture with products deployed to hundreds of thousands of users. He holds a BS degree in Engineering from the Indian Institute of Technology in Kanpur and additional degrees from the University of Massachusetts at Lowell.

FOUNDING TEAM

Atiq Raza
Co-founder & Executive Chairman
Virsec

Atiq Raza is an industry veteran, working in engineering leadership and senior management positions for the past 32 years. He served as Virsec's first CEO and now holds the position of Executive Chairman. He was the founder, Chairman and CEO of RMI, which was acquired by NetLogic, which Broadcom acquired on the strength of the RMI processor. Earlier, Raza was Chairman and CEO of NexGen, the first company to challenge Intel in microprocessors. NexGen became a public company and subsequently was acquired by AMD. Raza became the President and COO of AMD and served on its Board of Directors. He holds a Bachelor's degree in Physics from Punjab University, a BS with an Honors degree in Electrical Engineering from the University of London, and an MS degree in Materials Science & Engineering from Stanford University.

Ray DeMeo
Co-founder & SVP Business Development
Virsec

Ray DeMeo is a Co-Founder and SVP for Public Sector Business at Virsec. With over 20 years of operations and global business development experience, DeMeo has held critical roles in the successful growth and transition of multiple tech startups, including Giganet, acquired by Emulex and EqualLogic, acquired by Dell. He has led teams in roles of responsibility ranging from operations management to global sales and CEO. DeMeo holds a BS degree in Mechanical Engineering, a minor in Computer Science from Norwich University, and an MS degree in Business Management from Rensselaer Polytechnic Institute.

USP of VSP

Virsec is popularly known as a cybersecurity company to fully protect software as it is executing. Virsec's technology platform (VSP) defends against the widest range of known and unknown attacks, requiring no signature or prior knowledge. VSP also secures any and all critical business applications, from legacy and COTS to custom and modern, in any application workload in any environment, and with unprecedented speed and accuracy.

Additionally, Virsec claims it can protect the entire attackable surface of the application — including host, memory, and Web layers — during runtime. It enables businesses to consolidate their security infrastructure while reducing analysis time and labor.

The Early Adopter Phase

Many innovators face a major challenge when introducing a new and radically different technology into the market. The greatest challenge to overcome for any high-tech startup is from the early adopter phase to the early/late majority phase of the technology adoption lifecycle. The security industry has grown up understanding that the only way to attempt to secure against cyberattacks is to employ sophisticated algorithms, AI systems trained to detect malware, run pattern recognition, and predict behaviors.

Unfortunately, despite years of enhancing and expanding these methods, attacks have perpetuated, and hackers continue to refine and improve their level of sophistication.

"Because of the industry's continued failure to fully protect, our brand promise – to fully prevent cyberattacks – is occasionally met with disbelief. For us to build and sustain a remarkable business, Virsec must undertake the responsibility of shifting the industry's collective mindset and give credence to the fact that our customers can be fully protected from the most advance types of cyberattacks," says Dave Furneaux, Co-founder & CEO, Virsec.

The Funding

Virsec's initial seed funding came from angel investors, including Furneaux. Following the initial funding, they expanded the seed round to $3 million, allowing additional investment from investors such as Artiman Ventures, Boston Seed Capital, and a group of angel investors. Since then, Virsec has successfully raised $137 million in venture funding.

In June 2021, Virsec raised a $100 million Series C investment from a community of industry players and company builders, including former Chairman and CEO of Cisco, John Chambers, EMC's former Chairman and CEO, Mike Ruettgers, as well as several former high-ranking government and intelligence officials and investment firms. Led by BlueIO, the round also included Allen & Company LLC, Arena Holdings, Intuitive Venture Partners, JC2 Ventures, Artiman Ventures, Quantum Valley Investments, and Marker Hill Capital.

This seminal funding round will be used to continue to propel their growth engine. Furneaux articulated, "We're investing in expanding our go-to-market presence by hiring the best and most experienced talent in the industry. Additionally, we are strengthening our product development team to multiply our capabilities and continue to build a world-class security product that meets all enterprise and public sector customer needs and requirements. Our ample runway will allow us to fuel our growth through a future funding round or planned event."

Delivering Digital Transformation

CIOs and CISOs worldwide look to Virsec to provide them with better protection, reduce total cost of ownership (TCO), and increase their ease of compliance by filling critical gaps in their security programs. The VSP helps enterprise CIOs and CISOs deliver digital transformation and meet changing demands on application workloads with a solid security practice and protection assurance that stops threats at runtime and prevents dangerous attacks targeting applications and workloads most vital to business.

For Virsec, customer satisfaction is paramount; successful integration with the customer's existing environment and to provide full protection is their priority. Additionally, the feedback from the customer is a valuable resource that helps them improve the product offering as it gives them a platform to improvise and tweak as per the customer requirement.

"Some of the features that have been added are a result of the requests from customers or prospective customers. Leading a technology startup is a journey — we will never be finished and always will be a work in progress," opines Furneaux.

He added, "Defense contractors such as Raytheon and Lockheed tested our product extensively and eventually became a customer, our first commercial installations of any scale were with Broadcom and a U.S. Alliance Middle Eastern Government. Both were big successes and resulted in the expansion of our product being used across their critical software applications."

Accelerate and Innovate

The startup space is burgeoning with entrepreneurs waiting to create a niche with their unique service offerings.

Virsec views the total addressable market as potentially protecting every single server workload that exists in the world. It attributes its continued growth to its ability to accelerate within marquee enterprise and public sector accounts.

"When we raised our Series C funding, we reaffirmed our commitment to continue to innovate to meet the emerging demands of our customer and the evolving threat landscape," said Furneaux.

Virsec claims that it can converge critical workload protection capabilities in a single solution — including application control, system integrity assurance, and advanced memory and exploit prevention to protect the entire attackable surface of the application. This includes host, memory, web layers, and all runtime elements, whether on-premises, in the cloud, a container environment, or on a virtual machine.

Professional Competition

Multiple vendors offer solutions for protection, and according to Virsec, in the workload protection space, they have competition from EDR vendors. However, the company claims their tools lack the depth

of protection that VSP offers for server-side protection. This includes visibility into attacks during true runtime (as code executes) and the ability to ensure responsive action as events happen. Moreover, detection is based on problematic detection schemes that are rooted in AI and learning that requires analysis and results in numerous false positives.

"I keep hearing: There is no silver bullet for cybersecurity — no single solution that can address all security issues. Yet we have proven that there is a solution to stop the major cyberattacks that are plaguing governments, businesses and people across the world. My biggest fear is that Virsec is unable to achieve the mission we strive for — to make cyberattacks irrelevant," says Furneaux.

The company envisions a world where we remember ransomware, remote code execution, and other types of attacks as relics of the past. Certain obstacles and headwinds will prove to be challenging for them; however, they believe that their mission, over time, is attainable.

Making Cyberattacks Irrelevant

Virsec's company culture is defined by their shared belief that they are on a mission to make cyberattacks irrelevant. Dave Furneaux has articulated the company's virtues and values in a way that reminds every Virsec employee how truly meaningful and important their work is. The underlying philosophy, which guides all employees and how they conduct business:

- **Mission-driven:** Virsec was born to solve the problem of hackers plaguing the world. They are unwaveringly committed to opposing this evil, striving to protect others and never lose sight of that goal.
- **Zero Politics:** The notion of protecting against cyberattacks is an issue reaching beyond the bounds of politics. It is a matter that supersedes any faction, distinction, or partisanship debate. Virsec believes there is no room for politics — internal or external — which are merely a distraction from achieving the mission.
- **See Around Corners:** Intellectual curiosity fuels innovation. As Virsec redefines how software is secured, it believes in bettering through the pursuit of knowledge and learning. Having foresight and desire to evolve proactively is integral in defending the world from future threats.
- **Precision and Excellence:** As agents of change, we must hold ourselves accountable to the highest standards and quality to ensure trust within our community. This does not mean we do not take risks — we need to take bold risks — and make it safe to do so.
- **Accountable to the Family:** Enabling full protection is the lifeblood of Virsec. This includes protecting and supporting our people and stakeholders – employees, customers, partners, and community.

> Virsec's company culture is defined by their shared belief that they are on a mission to make cyberattacks irrelevant.

Fueling the Fire

It's nearly impossible to define the exact formula for what makes a startup successful; however, a number of factors kept the "fuel burning" at Virsec, and they all had to do with people.

According to Furneaux a successful company begins with assembling an excellent team. "The high-performance team we have brought together at Virsec has allowed us to build trust and support one another, strengthen our unified skillsets, and more effectively strive for our company's mission. Second, we have worked to create and nurture a community of stakeholders to support our growth and are involved in mutual collaboration."

I believe our community is one of our greatest assets. We've leveraged them to gain integral insights, provide business advice, orient fundamental feedback, and explore new business development. Lastly, I believe it is always important to embolden your company and employees to work to always see around corners."

Virsec has a well-established culture of intellectual curiosity. This has fueled their innovative spirit and given them foresight and the ability to evolve over time.

Advice to Aspirants

"I'm always inspired by the wisdom of Ray Dalio. One of his principles is, "It's more important to do big things well than to do small things perfectly."

Furneaux says, "At Virsec, we are taking on one of the world's most critical problems. Ending hacking and making cyberattacks irrelevant is more than a big, hairy, audacious problem – it's a moonshot mission. My advice for any aspiring entrepreneur is to find your moonshot. I believe successful companies cannot exist in the 21st century without being mission-oriented. Find a big problem, focus maniacally, and create a moonshot approach to solve it."

> Virsec Security Platform (VSP) stops sophisticated attacks at the first point of insurgence, so an adversary does not have the dwell time in software to orchestrate and execute their malicious plans. The solution eradicates threats to the software workload at runtime, in real-time, while reducing the cost of security operations.

KEY DIFFERENTIATORS

- Armed with an application awareness and runtime visibility, **Virsec Security Platform** claims it can detect and stop deviations caused by attacks that are invisible to conventional security tools.
- Virsec Security Platform® (VSP) provides continuous **application-aware workload protection** from inside the host. Unlike traditional tools designed for threat hunting and investigation, VSP focuses on ensuring system integrity, maintaining application control, and preventing advanced attacks like ransomware and zero-day events that allow actors to seize control of vulnerable workloads.
- **VSP employs a deterministic approach to detection**, built on patented AppMap technology that maps the trusted software stack across web, host, and memory layers and legitimate execution flow.
- **VSP solution delivers zero dwell-time defense** that counters threats upon inception or instantiation to prevent infection of server software components, memory-based attack staging and misuse of process control flow, Shellcode/batch files/web shell to persist and expand across networks.

KICKSTARTER

SNAPSHOT

Company Name
Virsec, Inc.

Product Name
Virsec Security Platform

Co-founder, CEO
Dave Furneaux

Co-founder CTO
Satya Gupta

Co-founder, SVP Bus. Dev.
Ray DeMeo

Co-founder, Exec Chairman
Atiq Raza

Website
https://www.virsec.com

https://www.linkedin.com/company/virsec-systems/

https://twitter.com/virsecsystems

https://www.facebook.com/virsecsystems

United States, India

Employees
160+

Awards

Distinguished Vendor TAG Cyber Security - Q3 2021

Cyber Defense Magazine Global Infosec Awards 2021

SC Awards 2021 Best Web Application Solution

Cyber Defense Magazine 2021 Global InfoSec Awards CTO of the Year

Enterprise IT World CIO Select Awards 2021 Server Workload Protection Award Winner

Security Today CyberSecured 2020 Enterprise Security Award

Industry-wise Services

Government & Defense, BFSI, Healthcare, Manufacturing, Education

Funding

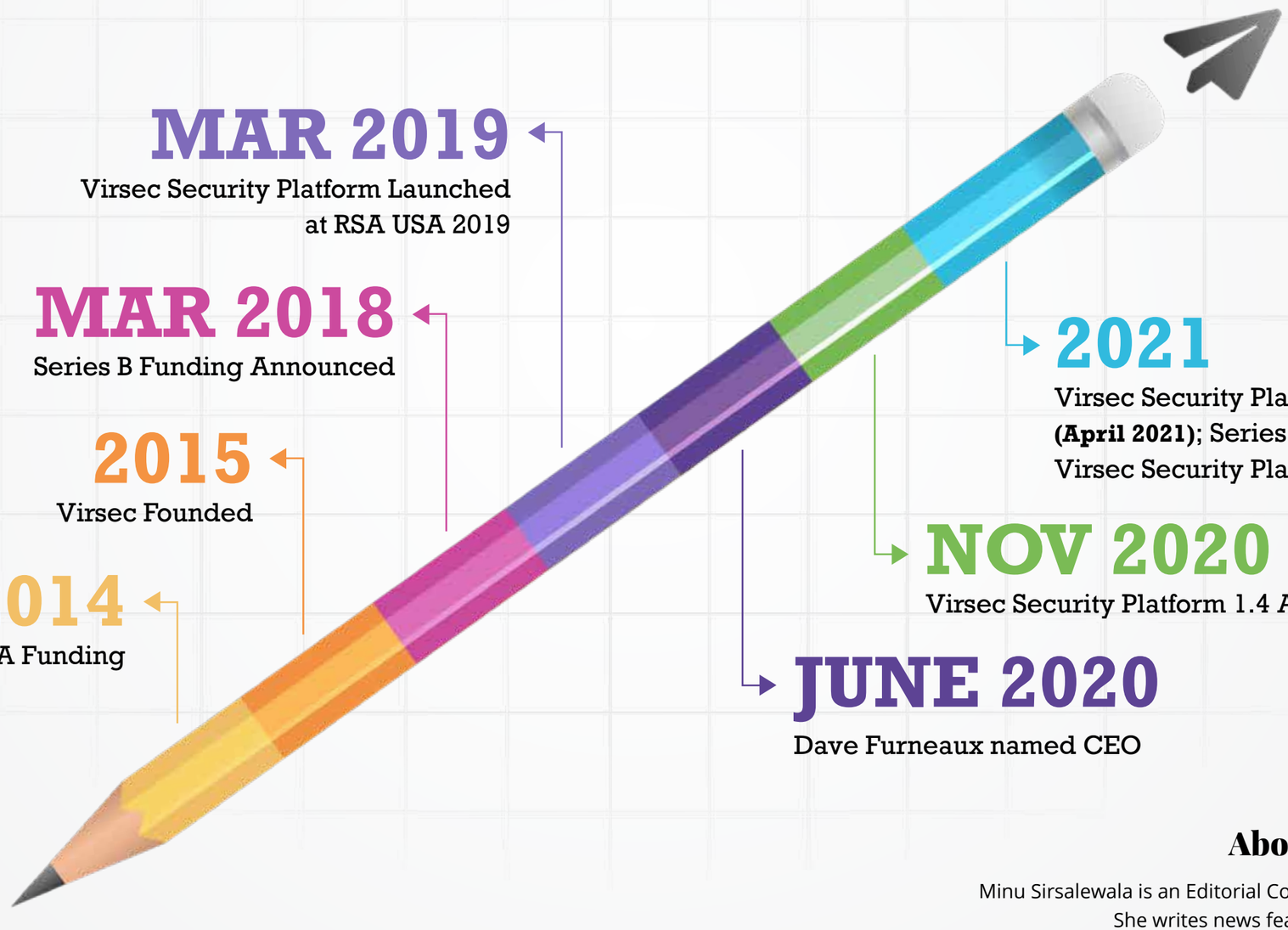
Series A Funding: Artiman Ventures, Tribeca Venture Partners, Boston Seed Capital

Series B Funding: Total Investment for Series B: $24 Million

Investors: Led by BlueIO, Artiman Ventures, Amity Ventures, Raj Singh, and Boston Seed Capital.

Series C Funding: Total Investment for Series C: $100 Million
Investors: Led by BlueIO, notable investors include Former Chairman and CEO of Cisco, John Chambers, Former Chairman and CEO of EMC, Mike Ruettgers, Allen & Company LLC, Arena Holdings, Intuitive Venture Partners, JC2 Ventures, Artiman Ventures, Quantum Valley Investments, Marker Hill Capita

COMPANY TIMELINE



MAR 2019
Virsec Security Platform Launched at RSA USA 2019

MAR 2018
Series B Funding Announced

2015
Virsec Founded

2014
Series A Funding

2021
Virsec Security Platform 2.0 Announced **(April 2021)**; Series C Funding **(July 2021)**; Virsec Security Platform 2.2 **(Coming Soon)**

NOV 2020
Virsec Security Platform 1.4 Announced

JUNE 2020
Dave Furneaux named CEO

About the Author

Minu Sirsalewala is an Editorial Consultant at *CISO MAG*. She writes news features and interviews.

STAY VISIBLE!

REACH OUT TO THE EVER GROWING GLOBAL INFOSEC COMMUNITY

ADVERTISE WITH US

CISO MAG
beyond cybersecurity

FOR MORE INFO WRITE TO
cisomag@eccouncil.org

230,000
Readership Reach
EC-Council & CISO MAG Combined

30,000+
Registered Readership
EC-Council & CISO MAG Combined

90,000
New Page Views

cisomag.eccouncil.org

CISO MAG

beyond cybersecurity

SCAN AND STAY UPDATED WITH
REAL TIME CYBERSECURITY NEWS