SPECIAL ADVERTISING SUPPLEMENT IN PARTNERSHIP WITH CAPITALCISO

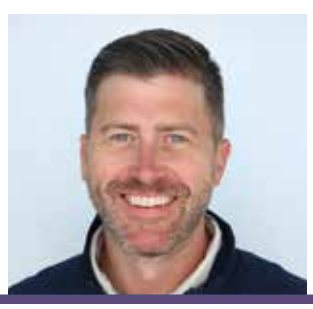
WASHINGTON
BUSINESS JOURNAL

2026

CAPITALCISO ORBIE® AWARDS

The annual CapitalCISO ORBIE® Awards honors chief information security officers who have demonstrated excellence in security leadership. Winners in the Global, Large Enterprise, Enterprise, Corporate & Healthcare categories will be announced June 25 at The Ritz-Carlton, Tysons Corner.

CAPITALCISO



FROM THE CHAIR

30 Capital CISOs beat executive isolation

PG 3

CONGRATULATIONS **2026 CAPITALCISO ORBIE NOMINEES**

JASON ALEXANDER
VCU Health

BENJAMIN AUCH
Gannett

RAJ BADHWAR
Jacobs

HEMANT BAIDWAN
U.S. Department of Homeland Security

DAVID BAKIN
Peraton

DIANE BALL
McCormick & Company

PAUL BECKMAN
ManTech

MIKE BEEKEY
Breakthru Beverage Group

DONNA BENNETT
U.S. Department of State

AARON BISHOP
U.S. Air Force

RYAN BOULAIS
Bunge

MARK BRAHLER
Modern Technology Solutions

ZACHARY BROWN
FDIC

GARY BUCHANAN
National Geospatial-Intelligence Agency

STACEY CAMERON
Halcyon Tech, Inc.

MANNY CASTILLO
Prince George's County

SPARTACO CICERCHIA
HMSHost

AMANDA CODY
Booz Allen Hamilton

ROBERT COX
The World Bank

ANDREW CUNJE
Appian

PAUL CURYLO
Inova Health System

RON DAVIS
ASRC Federal

JUSTIN DEPALMO
GDIT

KALEEM DIN
Creative Information Technology

MIKE DUFFY
U.S. Office of Management and Budget

VINIT DUGGAL
Intelsat US

ROB DUHART
Oracle

HEATHER DYER
United States Postal Service

JOE DYER
ICF

ELI EDELKIND
CAVA

WILL FARRELL
TikTok

MASSIMO FAVRO
NVR

ERICA FOWLER
United Bank

SEAN FRAZIER
Okta

MIKE GORDON
McDonald's

DONNIE GREEN
Anne Arundel County

CHERRI HEART
Carmax

AMY HERZOG
Amazon Web Services

ROBERT HUBER
Tenable Network Security

LINDA HUDGENS
Barclays

AARON HUGHES
AstraZeneca

DAVID INABINET
Riverside Health System

JOHN ISRAEL
KPMG USA

GRANT JEWELL
Northrop Grumman Corporation

JOEL JOHNSON
Lockheed Martin

LAWANA JONES
United Way

MATT KARNAS
UNFI

KENT KLING
TNS

DUC LAI
University of Maryland Medical System

HUGO LAI
Temple Health

MICHAEL LAVOREL
CareFirst BlueCross BlueShield

NATE LESSER
Children's National Hospital

BRUCE LIMING
Government Publishing Office

KOOS LODEWIJKX
IBM

STEVE LUKOSE
Sunrise Senior Living

ROY LUONGO
United States Secret Service

VIKAS MAHAJAN
American Red Cross

MATT MELLA
Iron Bow Technologies

RYAN MESSIER
Chemonics International

MEHRAN MOSBRIANTANHA
Personify Health

CJ MOSES
Amazon

DAVID NATHANS
Siemens Healthineers

JIM NELMS
Smithfield Foods

MIKE NEWBORN
Navy Federal Credit Union

VU NGUYEN
U.S. Department of Justice

CHRIS NIMS
Capital One

KYLE OETKEN
AES

ERIC PANKETH
SONY

KAT POFF
Calvert County Government

CHRISTOPHER PORTER
Fannie Mae

MATTHEW POSID
KPMG USA

MICHAEL PRAKHYE
Adventist HealthCare

RICHARD PUCKETT
United Health Group

DREW PULLER
MedStar

DANIELLE ROWELL
U.S. Office of Personnel Management

DARICH RUNYAN
Langley Federal Credit Union

ERIC SCHLESINGER
Parsons

KHAN SHAHAB
Airbus

PETER SILLITOE
Carlyle

ERIC SINCLAIR
Evolent Health Inc.

JOSH SOSNIN
Ellucian

SEAN STALZER
Dominion Energy

CHARLES STERLING
Host Hotels & Resorts

BOB TAYLOR
City of Baltimore, Maryland

GREG THOMPSON
VHC Health

DAVON TYLER
Federal Student Aid

KYLE WAGGONER
Perdue Farms

CASEY WATKINS
FTI Consulting

MICHAEL WATSON
Virginia Information Technologies Agency

DENNIS WEBB
Maryland Department of Human Services

CHRISTINE WHICHARD
IDEXX

BRIAN WHYTE
Deloitte

JR WILLIAMSON
Leidos

ERIK WINEBRENNER
Thermo Fisher Scientific

KEVIN WINTER
Deloitte

30 Capital CISOs beat executive isolation

Even the strongest executives can feel isolated at times. When chief information security officers (CISOs) face challenges with trusted peers, isolation transforms into clarity and confidence.

CapitalCISO brings together top CISOs from the capital's leading organizations to build meaningful relationships, share what's working, and create real business value. While industries and organization sizes may differ, the challenges of leadership—and the power of connection—are universal.

The Inspire Leadership Network connects CISOs with over 2,000 C-suite executives across more than 50 chapters, spanning public, private, and nonprofit organizations across North America. Beyond CISOs, Inspire also serves communities for chief information officers (CIOs) and chief marketing officers (CMOs).

For more than 25 years, the ORBIE Awards have honored C-suite executives for leadership, innovation, and excellence. I encourage you to attend the 2026 CapitalCISO ORBIE Awards to meet and support these outstanding technology leaders.

On behalf of CapitalCISO, congratulations to all nominees and finalists on these achievements. Special thanks to the awards partners, chapter underwriters, and staff whose support makes the CapitalCISO ORBIE Awards possible.

Sincerely,

Michael Baker
2026 Chair, CapitalCISO
VP, Global CISO, DXC Technology

GLOBAL **FINALISTS**

ORGANIZATIONS OVER $1 BILLION ANNUAL REVENUE & MULTINATIONAL OPERATIONS

Joseph Dyer

VP & CISO, ICF

Joseph Dyer serves as Vice President and Chief Information Security Officer at ICF. He has over 40 years of experience in information technology, including over 25 years specializing in information security. Widely known as "Mr. Cybersecurity," Mr. Dyer actively contributes to the cybersecurity community through speaking engagements, participation on professional panels, and mentorship of current and emerging practitioners. He holds a BS degree in Information Systems, published author, and achieved numerous industry certifications.

SUCCESS STORY: As a team, we delivered transformative advancements strengthening security by embedding automation and AI-driven capabilities into core operations. We also implemented a formal Continuous Threat Exposure Management (CTEM) framework, delivering broader enterprise-wide visibility into attack surface risk, reducing mean time to detect and resolution. Maintained key compliance objectives, including ISO 27001, CMMC Level 2, SOC 2, and NIST-based controls. Recognizing that modern cyber threats extend beyond any single organization, we embraced a "cyber village" concept, collaborating with industry partners and public authorities. This approach directly assisted in the pursuit of a large-scale fake-employee scam, demonstrating the power of coordinated defense.

Sean Frazier

Federal CSO, Okta

As Federal CSO at Okta, Sean acts as the voice of the CSO for Okta's federal business and is responsible for the security of the federal program inside Okta. Prior, Sean spent over 25 years working in technology and public sector security for companies including Duo Security, Netscape, LoudCloud/ Opsware, Proofpoint, Cisco & MobileIron. Sean helped lead numerous projects used by the DoD and Intelligence Community, including the Fortezza Crypto Card, Defense Messaging System (DMS), and others.

SUCCESS STORY: I lead the team that delivered a FedRAMP HIGH & IL4 authorization at the same time.

John Israel

Global CISO, KPMG

Global CISO at KPMG, with over 28 years of leadership experience across the Americas, EMEA, and Asia-Pacific. I lead cybersecurity strategy and operations across 135+ countries, with a deep specialization in AI, data security, and AI-driven defense. My work focuses on securing our global enterprise, AI adoption, protecting enterprise data, and aligning cyber risk to business growth. I co-authored a patent in secure optical communications and contribute to industry forums on AI & Data Security.

SUCCESS STORY: My greatest success has been partnering with KPMG's Trusted AI program to build a robust, enterprise-scale AI security architecture that enables innovation while protecting trust. Together, we established clear security foundations aligned to the Trusted AI pillars and operationalized security of, from, and with AI, integrating emerging technologies across data protection, monitoring, and assurance. This work transformed data security from a control function into a business enabler, laying the groundwork for increased velocity, efficiency, and creativity-allowing the firm to scale AI adoption confidently while managing risk in a rapidly evolving landscape.

Grant Jewell

Corporate Director & Deputy CISO, Northrop Grumman Corporation

Grant Jewell, CISSP, is a recognized thought leader in Cybersecurity with over 26 years of experience in IT and Cybersecurity, including 20+ years in management. Throughout the past two decades, he has helped shape NIST publications and influenced policies within the DoD CIO office. As the leader of a skilled team of cybersecurity professionals, Mr. Jewell successfully established global cybersecurity operations centers, managed critical application migrations, and represented Northrop Grumman at key external advisory forums.

SUCCESS STORY: My success story is the trust my team and Company have placed in me to deliver cybersecurity and resilience that enables our business to protect the warfighter. True success is driven not just by our technological advancements, but by the exceptional people behind them. I'm proud to serve Northrop for 25 years, from cybersecurity analyst to Deputy Chief Information Security Officer. My success is the honor to support product teams, coach talented individuals, and guide Northrop Grumman's CSOC from nascent capability to a recognized world-class team of cybersecurity experts that love what they do and will train the next generation.

Eric Schlesinger

CISO, Parsons

Eric Schlesinger currently serves as Chief Information Security Officer for Parsons Corporation, leading enterprise cybersecurity strategy, operations and risk management programs for a global mission-critical organization. In his role, Eric is focused on developing high-performing teams and scalable security programs built upon a foundation of people and processes with technology acting as the enabler. He is passionate about maturing proactive and predictive capabilities to best enhance resilience and enable secure business growth.

SUCCESS STORY: We transformed cybersecurity from reactive to proactive and predictive. Centered on identity, with extended visibility and applied intelligence and automation, we shifted from being alert-driven to predicting and disrupting risk before it reaches us. The outcome: a stronger, more resilient organization that can operate faster with confidence, securely navigating the most complex, high-risk environments without slowing mission or performance.

Peter Sillitoe

CISO, The Carlyle Group

Peter Sillitoe is the Chief Information Security Officer (CISO) at The Carlyle Group. He is responsible for shaping and leading Carlyle's global information security strategy, protecting the firm's data, systems, and technology assets.Peter has over twenty years of experience in cybersecurity and technology leadership across both government and private sectors. Prior to joining Carlyle, he led global cyber operations at Morgan Stanley; he also served in the UK's National Cyber Security Centre (NCSC).

SUCCESS STORY: Under my leadership, we modernized our technology landscape and shifted to proactive risk management. We deployed a modern endpoint stack and AI-enabled tooling across security processes, automating detection, response, and compliance monitoring while keeping human judgment at the center of decisions.This freed teams to focus on higher-value analytical work, improving efficiency and accuracy. We scale these capabilities with strong governance and control frameworks, ensuring innovation is disciplined and secure. Equally important, we reshaped our culture so cybersecurity is viewed as a shared responsibility and an enabler of innovation, strengthening organizational resilience, deepening trust, and increasing engagement across the firm.

AUGUST 4-6, 2026 | BAY AREA

Experience the power of connection with North America's top C-suite leaders at Converge26. Register today at **go.inspirecxo.com/C26.**

CONVERGE 26

LARGE ENTERPRISE **FINALISTS**

ORGANIZATIONS OVER $10 BILLION ANNUAL REVENUE

Mike Newborn

CISO,
Navy Federal Credit Union

Mike Newborn is Navy Federal Credit Union's Chief Information Security Officer, bringing more than 25 years of experience in cybersecurity and risk management. Passionate about technology, and the credit union mission of helping people, he previously led cybersecurity efforts at McKinsey & Company, Bloomberg's National Affairs and VeriSign. Mike also serves on the Cloudbreak Foundation nonprofit board aiding vulnerable populations in Washington DC, and other advisories like Blu Venture Investors Strategic.

SUCCESS STORY: I'm proud to have built a team that has fundamentally transformed how we identify, manage, and report risk, while enhancing our resilience in a challenging threat environment. We evolved our employee-based Phishing Test Program to address key threats through a fun, competitive, enterprise-wide approach. That program became a catalyst for meaningful dialogue on security topics at every level of the organization, including engagement with the board. Building this team and helping shift the company mindset in support of our digital transformation has been one of my most significant accomplishments.

Vu Nguyen

CISO,
U.S. Department of Justice

Vu T. Nguyen has played a critical role in shaping the future of the federal government's cybersecurity posture. He currently serves as CISO for the Department of Justice. Prior, he served as acting CISO at the Department of Homeland Security, U.S. Citizenship and Immigration Service, where he managed the component's cybersecurity defense initiatives. Nguyen holds a Master of Science in Telecommunications focused on cybersecurity and computer forensics from George Mason University.

SUCCESS STORY: Under Vu's leadership, his team delivered Department-wide progress in maturing the DOJ's Zero Trust Architecture through implementation of its three core pillars: identity provider - Okta, zero trust broker - Zscaler, and endpoint detection and response - CrowdStrike. He led the consolidation of Department applications to Okta completing 393 new application integrations, bringing the total to 996 applications protected by centralized identity controls, including 100 percent of Justice Management Division applications previously using weaker federated authentication. This effort significantly reduced the Department's identity attack surface and eliminated duplicative authentication systems.

Sean Stalzer

VP, Cyber Security & CISO,
Dominion Energy

Sean Stalzer is CISO, Vice President–Cyber Security at Dominion Energy. He has responsibility for working across the enterprise to establish and implement cyber security policies and practices to protect the company against an ever-evolving threat landscape from cyber criminals and hostile nation states such as China and Russia. Sean designed the cyber security program at Dominion on the philosophy that cyber security is a people challenge and not a technology problem.

SUCCESS STORY: Dominion Energy is 'the' first strike target in a war due to the reality that the brain of the internet lives in Northern Virginia. If it goes down, the entire world economy ceases to operate. As such, it is imperative to have an exceptionally strong cyber program to keep the energy to those data centers uninterrupted. With a turnover rate of under 1%, we have built a world leading cyber organization with deep government relationships, real time collaboration with intelligence agencies and DOW and exceptional business controls and relationships. The cyber security of today is not good enough for tomorrow.

Michael Watson

CISO (fmr.), Virginia Information Technologies Agency

JR Williamson

SVP & CISO,
Leidos

JR Williamson is the SVP and CISO of Leidos. In that role, he is accountable for all aspects of information security strategy, governance, risk, and full lifecycle cybersecurity operations for the corporation. Specific duties include the governance and defense of the corporation's computing environments: protection of unclassified and classified intellectual and digital assets against emerging cybersecurity threats; effective risk-based security policies, procedures, and operating practices; and development and retention of our cybersecurity workforce.

SUCCESS STORY: I started in this role nearly 8 years ago with the intent to learn what was important to the company with a productive sense of urgency to build a world class cybersecurity program. I then worked backwards to listen to the stakeholders of those plans and the providers and enablers of those outcomes to understand how to use my new team to earn trust through partnership, drive transformation throughout the company, establish the team that could grow and rise to those needed business outcomes, and build a culture of cybersecurity that enables business to execute better, faster, and safer.

ENTERPRISE **FINALISTS**

ORGANIZATIONS OVER $1 BILLION ANNUAL REVENUE

Paul Beckman

CISO,
MANTECH

Paul Beckman serves as the CISO of ManTech. Since joining ManTech in 2021, Mr. Beckman has drawn on extensive experience in government cybersecurity, previously spending 15 years as a Senior Executive at the Department of Homeland Security ending his career there as CISO for the Department. He holds numerous certifications, including CISSP, CCSP, MCSE, CCNA, CWNA, and CWSP. He earned a Master's in Project Management from GWU and a BS of Psychology from Radford University.

SUCCESS STORY: Under my leadership, our security organization evolved from siloed capabilities into an integrated, intelligence-driven risk management program aligned to mission outcomes. We built a next-generation platform that unifies technical, identity, and operational risk into a continuous, decision-ready view, shifting leadership from reactive compliance to proactive, data-driven decisions. We also leveraged AI to enhance detection, reduce noise, and scale operations without increasing headcount, while maintaining strong governance. Additionally, we modernized identity and access management, strengthening security and user experience. These efforts drove a cultural shift toward collaboration, innovation, and continuous improvement, positioning us for resilient, risk-informed cybersecurity leadership.

Ron Davis

CISO,
ASRC Federal

Ron Davis is seasoned cybersecurity executive and CISO with 25+ years of experience in federal and defense sectors. He currently leads enterprise cybersecurity at ASRC Federal and was previously the CISO at HII and Vencore. Ron's expertise is in cybersecurity strategy, governance, risk management, incident response, and compliance. Ron was a former BAE Systems leader managing global operations across 5 Home markets. He is known for building high-performing teams and integrating cybersecurity into business operations.

SUCCESS STORY: Our team's greatest accomplishment under my leadership was achieving full cybersecurity regulatory compliance through a complete re-architecture of our IT environment—while simultaneously maintaining operational continuity across the enterprise.Executing against the requirement, we redesigned the IT architecture, implemented new security controls, modernized identity and access management, strengthened boundary protections, and formalized governance processes. Simultaneously, we developed and institutionalized new IT processes to align with regulatory standards and industry best practices. We executed this transformation without disrupting core business operations. The resultant outcome was that we created a corporate culture that appreciates Cybersecurity as a core enabler to the business.

Donnie Green

CISO,
Anne Arundel County Maryland Government

Donnie Green Jr., a U.S Air Force veteran, serves as the Chief Information Security Officer (CISO) for the Anne Arundel County, Maryland government. In this capacity, Donnie is responsible for the strategic direction of enterprise cybersecurity functions and directly oversees all aspects of countywide cybersecurity operations, governance, risk and compliance, and incident response. Donnie has held various cybersecurity and IT leadership positions across federal, state, and local government.

SUCCESS STORY: My key achievement was leading a unified, highly effective organizational response to a recent county-wide security incident. Seamless cross-departmental coordination allowed our cohesive team to stabilized the environment and swiftly transitioned from containment to active recovery in just four days. The event served as a crucial real-world stress test of our systems and protocols. It resulted not only in the development of more resilient response procedures but also, and more importantly, forged a battle-tested team possessing the mutual support, collective knowledge, and confidence to effectively overcome any future challenges.

Vikas Mahajan

VP & CISO,
American Red Cross

Vikas Mahajan serves as Vice President and Chief Information Security Officer at the American Red Cross and has been with the organization for 10 years. Prior to the American Red Cross, Vikas served in IT management roles with AARP and PwC, architecting and implementing large-scale security solutions. He is a frequent speaker at industry podcasts, events and conferences and has written and contributed to books and articles on cybersecurity.

SUCCESS STORY: In 2024, following an executive tabletop exercise, I was asked to lead a resiliency program for our blood collections, manufacturing and distribution systems, which are responsible for more than 40% of the US blood supply. This resulted in massive reduction in our attack surface by more than 90% simply by removing VPN and remote access from those without a business need. Other highlights include network segmentation of the core blood system, immutable and/or airgapped backups for all critical blood systems, and business continuity planning with critical suppliers. For this effort, my project team was awarded a Red Cross Presidential Award.

Danielle Rowell

CISO (former),
Office of Personnel Management

Danielle Rowell is a cybersecurity executive with 13+ years of experience leading high-performing security organizations across the federal government. As Chief Information Security Officer at the U.S. Office of Personnel Management, she oversees enterprise cybersecurity strategy, AI governance, and cloud modernization efforts protecting data for millions of Americans. A certified coach and servant leader, Danielle is known for building resilient teams, driving innovation, and elevating cybersecurity as a mission-enabling business function.

SUCCESS STORY: During one of the agency's most turbulent periods, marked by significant organizational change and sizeable staff and budget cuts, my team sustained uninterrupted protection of HR, health, and retirement systems distributing $88B+ annually in federal benefits, with zero degradation to mission delivery.Key outcomes included $7.4M in cost efficiencies through tool consolidation and contract renegotiation, a modernized ATO process slashing approval timelines by 7–14 business days, and enterprise AI deployment to drive business efficiencies.Through servant leadership and relentless focus on mission, this team transformed cybersecurity from a reactive function into a resilient, mission-enabling capability — delivering innovation under extraordinary pressure.

Dennis Webb

Director of Cybersecurity, Maryland Department of Human Services

Dennis Webb has four decades of progressive experience in cybersecurity, information technology and management. As Director of Cybersecurity for MD DHS, his responsibilities encompass the full scope of a security executive, including developing and enforcing security policies, managing vulnerability and risk, and adherence to regulatory compliance requirements. He is recognized for his ability to translate complex business goals into effective strategies. Mr. Webb holds a Masters degree from Johns Hopkins University and a CISSP certification.

SUCCESS STORY: The Maryland Department of Human Services Cybersecurity Team successfully transformed from a gatekeeper into a mission enabler, building a culture of resilience. Integrating human capital strategy with cyber defense led to robust infrastructure improvements and innovative solutions. The team introduced a Risk-Informed Decision Framework that shifted us from "No" to "How," basing decisions on mission impact. This framework, supported by collaboration across all 54 locations and agency-wide education, fostered a critical security culture shift. This change lowered the risk of successful attacks, addressed the human element, and simplified adherence to federal mandates, Maryland statewide security policies, and industry-specific compliance standards.

CORPORATE **FINALISTS**

ORGANIZATIONS UP TO $1 BILLION ANNUAL REVENUE

Stacey Cameron

CISO,
Halcyon Tech

Stacey Cameron is Chief Information Security Officer at Halcyon, with over 20 years of experience leading cybersecurity, risk, and compliance initiatives across federal, DoD, and commercial sectors. She specializes in building scalable security programs that align with business growth. Stacey is passionate about mentoring and developing talent and actively volunteers with the Meyerhoff Scholars Program, supporting the next generation of STEM leaders.

SUCCESS STORY: Under my leadership, Halcyon's security program has evolved into a scalable, resilient function aligned with rapid business growth. I expanded security capabilities and led the realignment of responsibilities between IT and Security, ensuring functions are appropriately structured as the organization scales. We implemented a 24x7 virtual SOC to enable continuous monitoring and efficient growth. The team achieved SOC 2 Type II compliance, strengthened GDPR controls, enhanced third-party risk management, and advanced a data protection program. Looking ahead, we are leveraging increased automation to further scale operations, improve efficiency, and strengthen risk management as the business continues to grow.

Andrew Cunje

CISO,
Appian

Andrew Cunje is Chief Information Security Officer at Appian, where he leads global security across cloud, product, and corporate environments. He has scaled the organization 10x while enabling 30+ certifications, including FedRAMP High and DoD IL5, unlocking regulated market growth. Known for aligning security to business outcomes, he focuses on building secure, scalable platforms that enable enterprise and AI adoption.

SUCCESS STORY: Built a security program that transformed from a cost center into a growth engine.Scaled the organization 10x globally while enabling 40+ certifications, including FedRAMP High and DoD IL5, unlocking access to highly regulated markets which doubled revenue in under 4 years. Eliminated critical attack paths, automated compliance (actually), and embedded security directly into the platform. These efforts enabled significant revenue growth, expanded global market access, and positioned security as a key differentiator in enterprise and AI adoption.

Matt Mella

CISO,
Iron Bow Technologies

Matt Mella is the Chief Information Security Officer at Iron Bow Technologies. He leads the company's cybersecurity program across strategy, architecture, operations, incident readiness, and risk management, partnering closely with GRC and business leaders across the organization. Known for his practical leadership style and strong cross-functional relationships, Matt helps drive secure growth, operational maturity, compliance readiness, and thoughtful adoption of AI across the business.

SUCCESS STORY: My team has helped strengthen the cybersecurity posture of our enterprise environment while partnering closely with IT and GRC to design, build, and maintain a CMMC enclave for handling CUI. That work also required maturing our policies, processes, and procedures so they better align with both compliance objectives and day-to-day business operations.I have also worked to build stronger relationships across the business so security is seen as a partner, not an obstacle. As a result, business leaders regularly engage me for guidance on security decisions, customer discussions, and risk-related questions.

Ryan Messier

CISO (former),
Chemonics International

Accomplished leader focused on protecting the enterprise, managing risk, securing assets, responding to threats, and recovering from incidents all while supporting the business and staff on the front lines. I have worked across many industries in both large and small companies but in the end, my goal is always the same, to protect the enterprise and enable the business.

SUCCESS STORY: My team successfully recovered from a compromise by a nation-state-sponsored actor, stabilized the environment and slowly re-built our entire security stack, with modern AI-based tools and services, while supporting 6500 staff operating in over 90 countries and territories. As a result of our 18-month journey, we strengthened ties with our US and European Government clients and have been awarded some of their most sensitive projects. Along the way, we learned how to operate in some of the most contested and politically volatile areas in the world while protecting our people, equipment and data from threat actors.

Mehran Mosbriantanha

Chief Information & Security Officer, Personify Health

Mehran Mosbriantanha is Chief Information Officer and Chief Information Security Officer at Personify Health, where he leads enterprise technology, cybersecurity, cloud platforms, and intelligent automation supporting nationwide healthcare services. He has over 30 years of leadership experience, including senior leadership positions at NextGen Healthcare and Kindbody, and has led enterprise-wide SOC 1 Type 2, SOC 2 Type 2, and HITRUST R2 certifications. He holds CISSP and CCSP certifications.

SUCCESS STORY: Following the merger that formed Personify Health, I led the integration of multiple legacy technology and security environments into a unified enterprise operating model. Under my leadership, the organization achieved clean SOC 1 Type 2, SOC 2 Type 2, and HITRUST R2 certifications across the entire enterprise while deploying Zero Trust access for 3,000 users and launching governed enterprise AI capabilities. These initiatives strengthened customer trust, improved security posture across business units, reduced licensing costs by approximately $2.8M annually, and positioned technology as a strategic driver of growth and resilience.

Kat Poff

CISO & Deputy Director of Technology Services, Calvert County Government

Kathryn (Kat) Poff is the Chief Information Security Officer and Deputy Director of Technology Services for Calvert County Government. With over 25 years in public sector technology, she leads cybersecurity strategy protecting systems that support critical county and public safety services for approximately 1,400 employees. Kat mentors emerging professionals through the MS-ISAC, contributes to Maryland cybersecurity initiatives, and holds the CISSP certification.

SUCCESS STORY: One of our team's most meaningful accomplishments has been building Calvert County Government's cybersecurity program from the ground up. We established a structured program that supports every department and employee, grounded in sustainable policy, governance, and operational practices.A key success has been transforming cybersecurity awareness through gamification. We introduced contests, challenges, and short engaging videos that made security approachable and encouraged friendly competition across departments. This shifted cybersecurity from a compliance exercise to part of workplace culture, increasing reporting of suspicious activity and reducing phishing susceptibility while strengthening the County's overall security posture.

HEALTHCARE **FINALISTS**

HOSPITALS & HEALTHCARE ORGANIZATIONS

Jason Alexander

CISO,
VCU Health

Jason Alexander is the Chief Information Security Officer and Vice President at VCU Health, where he leads enterprise information security, risk management, and incident response for a large academic health system. With more than two decades of experience across healthcare, retail, academia, and aerospace, he is known for building resilient security programs, developing high performing teams, and advising executive leadership and boards on cyber risk, governance, and strategy.

SUCCESS STORY: Under my leadership, the information security organization rebuilt stability and direction after a prolonged absence of formal management, establishing enterprise programs in security, governance, risk, compliance, and incident response. We modernized identity systems by automating provisioning and deprovisioning aligned with Workday and Epic, replacing manual processes with a role based model that reduced risk and improved scalability. I re-centered the security strategy on core best practices, delivering a board approved security program that shifted the organization from reactive to risk informed. Most importantly, we built a high trust culture, reflected in zero staff turnover over the last three years.

Paul Curylo

VP & CISO,
Inova Health System

Paul Curylo is Vice President and Chief Information Security Officer for Inova Health System, with 25 years' healthcare technology leadership and 40 years' military experience. He leads resilient, values-driven teams that protect patient care and enable trust. Under his leadership, Inova advanced intelligence-driven cyber defense and industry collaboration, earning national recognition. He served as inaugural Chair of the Virginia Hospital and Healthcare Association Cybersecurity Committee and is a board member of the HIMSS Virginia Chapter.

SUCCESS STORY: In 2025, Inova Health System was recognized by Press Ganey, CMS, and Leapfrog for world-class healthcare delivery. Inova's cybersecurity team supported these outcomes by strengthening resilience through intelligence-driven attack surface reduction and proactive threat hunting, focusing defenses on what matters most to patient care. The CISO established a multi-disciplinary Joint Remediation Task Force to resolve persistent cyber hygiene risks in critical clinical and laboratory systems, improving security where modernization is not immediately possible. At Inova, cybersecurity is a shared responsibility—through partnership and collaboration, we safeguard trust, enable care continuity, and confront cyber extortion at scale.

Duc Lai

VP IT Security & CISO,
University of Maryland Medical System

I serve as Vice President of IT Security and Chief Information Security Officer at the University of Maryland Medical System. One of the largest employers in the state of Maryland, we provide over a quarter of all hospital care to our communities in Maryland. Additionally, I serve as Program Co-chair on the CapitalCISO advisory board. I am also an active contributor to the Maryland State Cybersecurity Council, MDHIMSS and the HSCC AI and Cyber Governance groups.

SUCCESS STORY: With the support of my amazing team and the leadership at UMMS, I successfully aligned our cybersecurity strategy with our business strategy allowing us to focus on top risks and make smart investments. This alignment makes cybersecurity strategy a part of our business strategy.I am very grateful to my team at UMMS for being proactive and highly-effective professionals who are laser focused. They are amazing at safeguarding the systems and data that are critical to providing the best care to our patients.

Nate Lesser

VP & CISO,
Children's National Hospital

Nate has spent over 25 years driving innovation at the nexus of technology and security, holding technical and executive positions in government, non-profits, and the private sector. As VP & Chief Information Security Officer at Children's National, he leads the team ensuring the security of hospital systems and patient information. Previously, he served as Deputy Director of the National Cybersecurity Center of Excellence at NIST. Nate holds degrees in electrical engineering and serves on several boards.

SUCCESS STORY: The success of the cybersecurity program at CN can be seen through the culture of cybersecurity at the hospital. A key initiative is the "code dark" protocol, which empowers frontline staff to respond effectively to ransomware incidents. This proactive approach has become a model for other hospitals, significantly improving our risk posture. Additionally, we have integrated cybersecurity resilience into the Business Continuity Plans (BCP) of all departments. Each BCP now includes a section on "how to operate through an extended downtime of a month or more." These plans ensure that our operations remain resilient and uninterrupted, even during prolonged incidents.

Michael Prakhye

CISO,
Adventist HealthCare

Michael Prakhye is the Chief Information Security Officer at Adventist HealthCare. Michael is an accomplished and results driven leader, with over 20 years of experience in IT and Information Security. Michael is responsible for developing and implementing strategies to protect the organization from cyber threats, as well as creating and maintaining a cybersecurity roadmap, aligning security initiatives with organizational goals. Michael is directly responsible for defining enterprise security strategies and fostering security-first culture.

SUCCESS STORY: Over the past 9 years, we have created a world-class cyber security program. My team has been successful at utilizing limited resources and creative thinking. As a team, we have remained resourceful and found ways to do more with less. We are supported by our senior executives, a clear roadmap that we have developed and strategic investments in solutions that we trust. As a result, we can now benefit from a solid cyber security program and partners. Our cybersecurity program enables the business by safely leveraging technology while protecting patient information, clinical systems, and the continuity of care.

Greg Thompson

CISO (former),
VHC Health

Greg Thompson is Chief Information Security Officer at VHC Health, leading enterprise cybersecurity strategy across clinical and business systems. He oversees security operations, identity, and Epic Security, aligning cybersecurity to patient care and organizational resilience. With experience across healthcare, data centers, and federal sectors, he builds risk-driven programs focused on measurable outcomes, strong governance, and operational excellence.

SUCCESS STORY: Under my leadership, cybersecurity evolved from a reactive, tool-centric function to a risk-driven program aligned to patient safety, operational resilience, and regulatory requirements. We strengthened identity and endpoint controls, improved visibility across IT and clinical environments, and established a multi-year roadmap focused on incident response and recovery. These efforts reduced risk, clarified ownership, and positioned the organization for sustained maturity.

CAPITALCISO WHO'S **WHO**

ADVISORY BOARD OFFICERS

CHAIR
Michael Baker
DXC Technology

VICE CHAIR
James Saunders
State of Maryland

MEMBERSHIP CHAIR
Paul Curylo
Inova Health System

MEMBERSHIP CO-CHAIR
Nate Lesser
Children's National Hospital

PROGRAMS CHAIR
Duc Lai
University of Maryland Medical System

PROGRAMS CO-CHAIR
Amy Howland
Guidehouse

AWARDS CHAIR
Tammy Hornsby-Fink
Federal Reserve System

ADVISORY BOARD MEMBERS

Amit Chaudhary
Rolls Royce

Andrew Cunje
Appian Corporation

Grant Jewell
Northrop Grumman

Matt Klaus
AARP

Chris Lanzilotta
The Home Depot

CAPITALCISO MEMBERS

FRANK AIELLO
Maximus

DAVID BAKIN
Peraton Inc.

PAUL BECKMAN
MANTECH

MARK BRAHLER
Modern Technology Solutions

JASON BROWN
HII

CAREY CARTER
CNA Corp

RON DAVIS
ASRC Federal Holding Company

CHRISTOPHER DIAS
LMI

DUSTIN FRY
SageNet

ZACH FURNESS
The MITRE Corporation

JOHN ISRAEL
KPMG

MICHAEL KINNEY
Systems Planning and Analysis

JOHN MCCLURE
Sinclair, Inc.

MATT MELLA
Iron Bow Technologies

MIKE NEWBORN
Navy Federal Credit Union

CHRISTOPHER PORTER
Fannie Mae

MICHAEL RAEDER
Rocket Software Inc

DAN SADLER
Constellation

ERIC SCHLESINGER
Parsons Corporation

GREG THOMPSON
EdgeCore

ARNO VAN DER WALT
Humana

CAPITALCISO ORBIE AWARDS

Get involved with the ORBIE Awards:

THANK YOU TO THE 2026 CAPITALCISO ORBIE AWARDS PARTNERS

PRESENTED BY

CAPITALCISO | FORTINET | halcyon

SPONSORED BY

WASHINGTON BUSINESS JOURNAL
MEDIA PARTNER

Year Up United
NATIONAL PARTNER

Chainguard

Abnormal | okta | WIZ | zscaler

Bricklayer AI | CYERA | betweenpixels. | ELISITY

GUIDEPOINT SECURITY | LevelBlue | netskope | RSM