The Richmond Cyber Security Forum

The Pillars of a Conference

KEYNOTE SPEAKERS
Start the event with a bang - hear from the latest experts in fields that will expand your mind

INDUSTRY EXPERTS
Hear from those who are doing it themselves and pick their brains in an interactive and solution oriented setting

VENDOR PRESENTATIONS
Tangible re-world examples of potential solutions to your current problems

DISCUSSION GROUPS
Peer-led presentation-free conversations about the pressing topics of the day, the experiences people have had and the questions that keep them up at night

PROFESSIONAL DEVELOPMENT
Acquire the personal and professional skills that often get neglected

Col. Chris Hadfield

Astronaut and Former Commander of the International Space Station

Called "the most famous astronaut since Neil Armstrong," Colonel Chris Hadfield is a heavily decorated astronaut, engineer, and pilot who has become a worldwide sensation. His rendition of David Bowie's "Space Oddity" has been seen by over 75 million people and was called "possibly the most poignant version of the song ever created" by Bowie himself. Hadfield is a uniquely experienced leader who shares best practices and tactics on leading teams through complexity and change, while also sharing the marvels and wonders of science and space to everyone he encounters.

Formerly NASA's director of operations, Hadfield spent more than three decades working for NASA and the Canadian Space Agency. Throughout his distinguished career, he has flown three space missions, built two space stations, performed two spacewalks, crewed the Shuttle and Soyuz, and, in 2013, commanded the International Space Station for six months. His many awards and recognitions include the Order of Canada, the Meritorious Service Cross, and the NASA Exceptional Service Medal.

Hadfield is acclaimed for making outer space accessible to all. His keynote presentations have been called "an astonishing display of visual storytelling" by Harvard Business Review, and his TED talk "What I Learned from Going Blind in Space" has been viewed more than 11 million times. He is frequently featured on national and global media outlets and is the co-creator and host of the internationally acclaimed BBC series Astronauts: Do You Have What It Takes? as well as the co-host of National Geographic's One Strange Rock, directed by Darren Aronofsky.

Currently an adviser to SpaceX and Virgin Galactic, Hadfield was asked to advise and assist King Charles III in exploring sustainability in space in 2023. He is also an adjunct professor at the University of Waterloo and chair of the board of the Open Lunar Foundation.

Our Cyber Security Workforce is a Critical Infrastructure

Joyce Hunter
Former Deputy CIO, Policy and Planning, USDA and Current Executive Director, ICIT

Far too many associate cyber security with technology and an inherently technical field, and in doing so, they do a disservice to themselves, impair their comprehension of the landscape, and invalidate the troublingly few cyber security professionals tirelessly fighting to ensure the security and resilience of critical infrastructure. Cyber security has always been and will always be a "people problem" as much or more than a "technology problem."

Join Joyce Hunter as she discusses the US cyber workforce as critical infrastructure upon which all other sectors depend, and it is incumbent upon us to:
- Recognize it as such
- Actively collaborate to improve it
- Compensate skilled personnel proportional to the security and resilience they facilitate
- Work together to ensure that opportunities to enter or advance within the cyber workforce are inclusive, equitable, and available to all potential candidates.

Joyce Hunter is a strategic-doer and a philanthropreneur. She was appointed by President Barack Obama to the position of Deputy Chief Information Officer for Policy and Planning at the Department of Agriculture (2013-2017) and was the Acting Chief Information Officer from March 2016 to July 2016. Ms. Hunter is currently the Executive Director of the Institute for Critical Infrastructure Technology (ICIT), a non-profit Think Tank, providing objective, nonpartisan research, advisory, and education to legislative, commercial, and public-sector cybersecurity, national security and critical infrastructure stakeholders.

Virtual Battlegrounds:
Decoding the Cybersecurity Strategies of Nations

Zach Lewis,
CIO and CISO, University of Health Sciences and Pharmacy

Journey into the heart of digital warfare as this presentation on nation-state actors in cybersecurity explores the cyber capabilities and histories of prominent countries like Russia, China, Iran, Israel, the USA, and North Korea. The focus will be on detailing the development of their cyber capabilities over time. The analysis will extend to discussing the most prolific hacking groups associated with these nations, highlighting their notable activities. Additionally, we will delve into the examination of well-known and complex cyber-attacks attempted by these countries, while providing insights into the methodologies employed.

The presentation will also cover areas of interest for cyber sabotage or theft, offering a comprehensive view of the strategic cyber objectives pursued by these nation-states. By addressing the historical evolution, key hacking groups, and notable cyber incidents, this presentation aims to provide a nuanced understanding of the diverse approaches and motivations shaping the cybersecurity landscape on the global stage.

Zach Lewis currently serves as the CIO and CISO for the University of Health Sciences and Pharmacy. Zach has responsibility for the company's information technology strategy and cybersecurity operations, while also serving as the Enterprise Risk Management chair. He volunteers on IT advisory boards for SIUE and UMSL and is an officer in the St. Louis Chapter of InfraGard. Zach holds a CISSP, CRISC, CISM, CISA, and CGEIT as well as numerous other IT certifications. He was a recipient of Cyber Defense Magazine's Top Global CISOs of 2022 and 2023 and was named 40 Under 40 Security Leaders by CDO Magazine. Zach provides his industry expertise to others by speaking at conferences, webinars, and universities throughout the country.

Make Decisions Like a Fighter Pilot

Jim Covington
VP of Information Security and Privacy
SomaLogic

Since the 1960's the U.S. military and fighter pilots have utilized a decision-making method called the OODA Loop. This method focuses on making split second decisions and taking action with available information by continuously iterating through Observation, Orientation, Decision, and Action (OODA). The premise of the OODA Loop is to disrupt your "adversary's" decisioning by denying their common assumptions. Based on psychological, military, mathematical and philosophical principles, and developed by an Air Force Colonel, it resulted in a marked improvement in aerial combat success during the Vietnam war. But how does making better decisions in air-to-air combat relate to cybersecurity? Using real life examples, this talk will provide insight into how we can leverage the OODA Loop method to make better decisions, respond more quickly to events, and reduce failures in cybersecurity.

Jim Covington is a cybersecurity professional with 25 years of consulting and industry experience. Jim is currently VP of Information Security and Privacy at a leading proteomics BioTech company. Previously, he was Senior Associate at Booz Allen Hamilton where he was responsible for supporting clients through technical oversight of U.S. government critical infrastructure programs. Jim's experience includes building and leading a cybersecurity and data privacy program for a wireless health company and leading the cybersecurity compliance program focused on data privacy, protected health information, and credit card data for a global technology company. As a consultant, he has provided a wide range of industry and government clients with subject matter expertise for risk assessments, secure architecture, security policies and standards, education and awareness, and cybersecurity operations. Jim has been a speaker and panelist at regional and national cybersecurity and privacy events and has authored and co-authored numerous articles in peer-reviewed journals.

Redefining Security:
Embracing Zero Trust, Secure Service Edges, and the future of networks

Alex Green
CISO, Delta Dental Plans Association

In this session, we delve into the transformative world of cybersecurity, focusing on the pivotal concepts of Zero Trust, Secure Service Edge (SSE), and the strategic elimination of outdated technologies such as VPNs. We begin by exploring the Zero Trust framework, an approach operating on the principle of "never trust, always verify", ensuring rigorous identity verification for every user and device attempting to access resources on a private network, regardless of their location. We will cover how this concept has expanded to the enterprise concept of the Secure Service Edge, which amalgamates comprehensive security solutions to protect data and resources in a cloud-centric environment. This segment emphasizes how SSE can effectively safeguard users, devices, and applications, mitigating the risks associated with remote workforces and cloud-based assets. Finally, we address *how* this transformation takes place, supporting phasing out legacy technologies. We discuss the vulnerabilities inherent in these outdated systems and present modern alternatives that offer enhanced security, scalability, and user experience.

Join us for an enlightening journey through these pivotal cybersecurity strategies, crucial for business executives and cybersecurity professionals striving to fortify their digital infrastructures against contemporary threats.

Alex Green, a distinguished Chief Information Security Officer, is celebrated for seamlessly merging cybersecurity initiatives with business objectives. Serving as the CISO at Delta Dental Plans Association, he spearheads the creation of a comprehensive security strategy, rallying diverse security teams towards a unified business mission. Drawing from his rich background at DST Systems and H&R Block, Alex demonstrates exceptional proficiency in overseeing cybersecurity operations and managing engineering teams.

Beyond his corporate success, Alex is a proven entrepreneur who co-founded Kanshi and now contributes as a venture partner at The Veteran Fund. In this role, he collaborates with federal entities and startups, driving forward innovative cybersecurity solutions. Alex's journey in the US Army's Special Operations, specializing in electronic exploitation, underscores his adeptness in managing high-stakes security scenarios and unwavering commitment to national security.

Core Principles and Challenges of Leadership in Business

MK Palmore
Former Assistant Special Agent in Charge
F.B.I.

Leadership, a critical determinant of organizational success, is multifaceted and evolving. Contemporary leaders must know how to navigate these ever-changing complexities, including technological disruptions, managing diverse and remote teams, fostering a culture of continuous innovation, and addressing the growing emphasis on corporate social responsibility.

This session is essential for current and aspiring leaders who wish to leave a lasting impact in their organizations and industries, and will pivot around:

- Key principles that constitute effective leadership, including vision articulation, ethical decision-making, emotional intelligence, and adaptability in a rapidly changing business landscape.
- Case studies and real-world examples that illustrate how successful leaders are overcoming these obstacles.
- The importance of a leader's ability to balance stakeholder expectations with the company's strategic goals. We will also discuss the critical role of resilience and agility in leadership, especially in times of crisis or uncertainty.

Join MK Palmore, Former Assistant Special Agent in Charge at the FBI, as he guides participants to develop and hone their leadership skills to effectively navigate the complexities of the modern business environment.

MK's illustrious journey began at the United States Naval Academy, leading to a distinguished role as a commissioned officer in the U.S. Marine Corps. His deep commitment to public service was further solidified through 22 years with the Federal Bureau of Investigation (FBI). During his tenure at the FBI, he demonstrated exceptional skill and leadership in various domains, including counterterrorism, intelligence, risk advisory, white-collar crime, and, notably, cybersecurity. As the head of one of the FBI's largest cybersecurity teams in the San Francisco Bay Area, MK left an indelible mark on the field.

Transitioning seamlessly into the private sector, MK continued to showcase his expertise and leadership acumen. He played pivotal roles at two major technology corporations, including Palo Alto Networks and Google Cloud, guiding large-scale enterprises in their cloud transformation initiatives. Apart from his professional endeavors, MK is also a noted author and the host of The Leadership Student Podcast. His commitment to leadership, diversity in technology, and veteran career support reflects his holistic approach to making meaningful contributions across various domains.

EU and USA Regulatory Challenges for AI Usage

David Shapendonk
Chief Technology Officer at Maestro Games

AI and machine learning technologies have become integral to many applications and services within all industries and a key driver toward profits and innovation; however, AI also poses significant risks, including lack of transparency and explainability, over-reliance on AI, bias, and discrimination, vulnerability to attacks, lack of human oversight, high cost, and privacy concerns.

The European Union (EU) has taken the lead in proposing the EU AI Act, which is the first regulatory framework that establishes clear guidelines for companies developing and deploying AI systems based on the level of risk they pose. The EU's risk-based framework for AI regulation aims to support trustworthy artificial intelligence that is safe, transparent, and respects existing law on fundamental human rights.

The highest-risk AI applications must pass a conformity assessment by complying with a range of requirements, including risk management, testing, technical robustness, data training and data governance, transparency, human oversight, and cybersecurity. Developers of lower-risk AI must also meet transparency obligations to inform users when they are interacting with chatbots or AI systems that generate or manipulate image, audio, or video content. While the United States currently lacks comprehensive regulations, it will likely follow the EU's lead soon as pressure mounts to regulate AI.

The rise of AI regulation will significantly impact how technology vendors and users leverage machine learning and other AI capabilities in products and services.

David Shapendonk has worked for over 30 years on technology systems development and cybersecurity in the Entertainment and Life Science Industries. With a focus on artificial intelligence, machine learning, and virtual technology over the last 4 years. He is a Business Management & Industrial Relations graduate from Kwantlen Polytechnical University and hold a CISSP from ISC2. David also volunteers as a CISSP exam content developer for ISC2.

Ensuring Meaningful Cyber Spend: Let's Go Back to the Beginning

Bill Holmberg
IT Director, Wayne Transports, Inc

We are in a world where cyber-attacks are skyrocketing, but we are professionals are being asked to do more with less. How do we approach understanding what is critical and what is unnecessary legacy or lipstick on a pig? How do we combat complex threats with lean budgets and teams? How do we know which vendors will give us the greatest impact for our spend?

We get caught up in the latest fads and threats that sometimes we need to remind ourselves where we started. Join Bill Holmberg of Wayne Transports, as he slows the hype train down and re-emphasizes the importance of the basics:

- Reviewing the fundamentals & assessing the company needs
- The basics of a creating security plan
- 2024 Vendor overview
- Technology recommendations against a system attack

+ an Interactive tabletop exercise!

Bill Holmberg is the IT Director of Wayne Transports, Inc., since 2014, which services customers in all 48 states and Canada with 24/7 dispatch. He oversees the technology group, sets strategy initiatives, and oversees data back-up for the firm. Bill formerly supported and strategized IT for Endres Processing (2008-2014), he was the CTO and partner of The Hart Ski company (2003-2008), as well as the IT Director of Tech-Logic Corp- a library automation company- from 2002-2004. Previously he was the SAN manager at CH Robinson Worldwide from 2000- 2002, and the Onsite Support Manager and Macintosh Technical Lead for Imation from the mid-nineties through the Y2k events. Bill is an engaging speaker and presenter, performing stints at Metro State University for the Security And Forensics Education (SAFE) classes which was focused on helping Law Enforcement (LEO) and Banks and Non-Profits understand security and how it relates to their overall work and safety.

Bill is an Army Veteran, an accomplished musician and entertainer, and has performed in North and South America and many vacation destinations outside of the USA. Among his passions is hosting benefits, for any worthwhile cause.

The Power of Pressure:
Nail the Moments that Matter

Dane Jenson
CEO, Third Factor

How we navigate periods of intense pressure has a huge impact on how successful we are in our careers, how much we enjoy the journey, and how much regret we carry. Your ability to be successful as a senior leader depends directly on your relationship with pressure.

In this session, author and keynote speaker Dane Jensen will introduce practical strategies for using pressure as an advantage. Drawing insights from his book, The Power of Pressure: Why Pressure Isn't the Problem, It's the Solution, Dane will share unforgettable stories of pressure, explore practical skills for performing in peak moments and over the long haul, and leave you with renewed energy for tackling the biggest sources of pressure in your life.

You'll learn how to use the 'pressure equation' of importance, uncertainty and volume to anticipate and prepare for pressure; nail the peak pressure moments that can make or break a big sale, crucial meeting, or define a career; and maintain energy and motivation through long periods of sustained pressure to emerge with satisfaction and free from regret.

Dane Jensen is an acclaimed speaker, media commentator, educator and author.
He is a top-rated instructor at the University of North Carolina at Chapel Hill and Queen's University in Canada, and has contributed to the development of thousands of leaders in companies of all sizes through his company Third Factor.

In addition to his corporate work, Dane works extensively with coaches, athletes, leaders, and Boards throughout the Olympic and Paralympic sport system to enhanced competitiveness.

Dane is a regular contributor to Harvard Business Review. His work has been featured in The Wall Street Journal, Forbes, Strategy+Business, and countless others, and he was named a top virtual speaker by Entrepreneur magazine.
Dane's book, The Power of Pressure: Why Pressure Isn't The Problem, It's The Solution, was called "the best book I've read on pressure and performance" by championship-winning NBA head coach, Nick Nurse.

Safeguarding the Future of Innovation and Creativity with Generative AI

Tanweer Surve

Executive Director, Cloud Control
Management, Wells Fargo

Artificial intelligence (AI) and Machine learning (ML) have long been transformative forces in business, revolutionizing operations and decision-making. However, the emergence of Generative AI marks a new age requirement, as it goes beyond analysis to create new and original content, opening unparalleled opportunities for innovation and creativity.

Business leaders cannot afford to stand on the sidelines as generative AI reshapes the function of the future. Embracing this technology is crucial to maintaining a cutting-edge within your organization.

Join Tanweer Surve of Wells Fargo as he explores benefits and the unique or heighten existing risks needing to be managed throughout all stages of GenAI model onboarding, customization and use.

Strategic and delivery-focused senior technology leader, Tanweer brings deep subject matter expertise in the areas of Cloud Transformation, Cybersecurity, Artificial Intelligence and Governance, Risks & Compliance (GRC) management.

Tanweer has over 20 years of proven track record in IT & Business, executing various leadership roles and delivering large-scale complex Global Digital Transformation Programs across various parts of the world with his Technical and Business Management expertise in Enterprise Architecture, Cloud Technologies, and Cybersecurity.

Tanweer holds an MBA in Business Development and a Bachelor's in Engineering with a major in Fiber Optics Telecommunication.

THE REALITY OF ZERO TRUST

Although Zero Trust has gained widespread acceptance as a cybersecurity best practice in response to evolving threats and changing network architectures, it is not without its challenges and potential downsides.

This discussion group is ideal for sharing real-world experiences and innovative strategies that bolster the resilience of organizations in the face of sophisticated cyberattacks while exploring the challenges and pressures faced when implementing.

SECURITY 2024

Our annual conversation of all things concerning the security world, and the solutions to keep them at bay. Uncover new ways to look at old problems, new problems that require new solutions, and discuss the vendors that promise everything in-between.

Bring your questions for your peers to discuss, as a shared experience in a constantly evolving issue will give us the edge in this crucial battle.

CYBER SECURITY AND THE SUPPLY CHAIN (SHARED)

Chief Information Security Officers, Supply Chain Managers, and Logistics experts converge in this discussion group to address the escalating threats that cyber vulnerabilities pose to global supply chains. The group will discuss the importance of implementing robust cybersecurity measures to safeguard sensitive data, critical infrastructure, the seamless flow of goods and fortifying supply chain networks against cyber threats.

As cyber-attacks increasingly target supply chain vulnerabilities, join together to share best practices, exchange threat intelligence, and collectively bolster the cybersecurity resilience of supply chain and logistics operations worldwide.

The *Richmond* Cyber Security Forum

THOUGHT LEADERSHIP

TANGIBLE ADVICE

PEER NETWORKING

EFFICIENT VENDOR SOURCING

A TAILORED EXPERIENCE

All of this adds up to a productive 5-star experience that is created just for you, based on your needs and preferences.

To request an invitation, email Dana at
DSamuels@richmondevents.com