12TH ANNUAL ISSA-COS Cyber Focus Week (CFW) 2025 Speaker Biographies, Presentation Topics, and Abstracts

Opening Keynote Address: AI and Social Engineering

Abstract:

This innovative talk challenges your thinking about the state of security. We, as a community, have focused so much on raising awareness of security threats that we have neglected preparedness of those very same threats. Awareness is understanding car accidents happen. Preparedness is why you wear your seatbelt. In this talk we will discuss cyberpsychology, AI, deep fakes, and what it will take for us, as humans, to develop our "security seat belt" to prepare ourselves for these advanced attacks.

Presenter: ***Erik Huffman, PhD, Cyberpsychologist***

Dr. Erik J. Huffman is a cybersecurity researcher, cyberpsychologist, TEDx speaker, and host of the MiC Club podcast. His pioneering research in cyberpsychology has begun to uncover biological deficiencies in humans that function for survival in face-to-face interactions but do not activate in a cyber environment. These vulnerabilities allow cyberattacks, such as phishing and digital social engineering, to continue to thrive even as awareness grows. People are often the weakest link in the cyber environment, and Dr. Huffman is working to explain how the problem persists and what can be done to mitigate.

Generative AI vs. Human Psychology

Abstract:

It's widely known that in February of 2024, scammers tricked an executive in Hong Kong to send nearly $26 million out of his company. But have you ever thought about what went wrong from a psychological standpoint?

We'll take a human-centered look at what went wrong in Hong Kong and how things like cultural norms, financial industry standards, and cognitive fatigue created rich vulnerabilities for attackers to exploit. We'll also look at lesser-known generative AI case studies from a UK energy company, the world's biggest ad firm, and a well-known car maker. Most importantly, we'll walk through the human-based defenses that you can use to defend against these threats.

Presenter: ***Danika Hannon***

After following the cybersecurity industry for nine years, Danika Hannon started formally studying for a cybersecurity master's degree in 2023 and graduated in December 2024. In analyzing emerging threats, Hannon relies on IARPA's threat intelligence framework of figuring out who the threat actor is, what motivates them, what they're targeting, and how they're doing it. With that information in place, Hannon focuses on sharing guidance with both business and technical communities so that leaders can stay a step ahead of threat actors.

Establishing Artificial Intelligence Ethical Trust

Abstract:

Generative Artificial intelligence has introduced business opportunities for new markets and operational efficiencies. Along with these opportunities come new ethical challenges for organizations, where new innovations out-pace industry and legal standards. The lack of corporate governance leads to liabilities related to privacy, intellectual property, copyright, and discrimination.

This session will present ethical categories associated with artificial intelligence, vulnerabilities and technical limitations leading to corporate ethical liabilities, and guidance for establishing corporate governance to establish trust with AI-integrated business services.

Presenter: Eric Nordberg

Eric Nordberg serves as a security control integration risk assessor for a national healthcare organization. Eric has 20 years of IT governance, security, risk and compliance experience. Eric is a board member with the Pikes Peak ISC2 chapter. Eric's certifications include Certified Information System Security Professional (CISSP), Certified Cloud Security Professional (CCSP), and Certified Information Systems Auditor (CISA).

Current Cybersecurity Trends and the Evolving Role of Artificial Intelligence (AI) to include Defending Against Emerging Threats

Abstract:

A panel discussion on USSS's current general cyber trends we're seeing for 2025 and then evolve into AI and how it's playing a part and how we can use it on our side.

Presenters:
Derek Booth
Jared Labato

ATSAIC Derek Booth

Assistant to the Special Agent-in-Charge (ATSAIC) Derek Booth is one of the founding members of the Mountain West Cyber Fraud Task Force (MWCFTF) in Denver, Colorado, which began in 2012. The MWCFTF consists of 200+ members of federal, state and local law enforcement, network security, private business, and academia partners, and whose mission consists of supporting our partners and region in all cybercrime investigations including Ransomware, Network Intrusions, Business Email Compromise, and Computer/Cellphone Forensics. Derek became a Forensic Examiner of computers, cellphones, and skimmers in 2012 after spending his first 13 years on the job protecting a plethora of dignitaries including President George W. Bush and family full-time. Derek is originally from St. George, Utah, graduated from Southern Utah University with a Master's in Accounting.

NIFA Jared Lobato

With a tenure spanning 15 years in law enforcement and digital forensics, Network Intrusion Forensic Analyst (NIFA) Jared Lobato's journey culminated in his current role as a Network Intrusion Forensic Analyst with the United States Secret Service. This position allows him to delve deeply into the intricacies of digital crime, encompassing activities such as digital forensic analysis, mobile data recovery, and malware analysis/identification. Jared supported various local, state, and federal agencies, bringing to the table his expertise in both detailed lab evaluations and on-the-ground analysis of computer systems and networks. Internationally, Jared has taken his knowledge across borders, teaching on subjects like cyber exploitation in El Salvador, network investigations in Mongolia, and digital evidence for judges in Hungary. A consistent thread in his work has been his focus on financial crimes, to include network intrusions and skimming. Jared holds a Master of Science degree in Information Systems with a specialization in Cybersecurity, and an undergraduate B.S. in International Business/Finance.

Afternoon Keynote Address: How Israeli Military Intelligence is Developing the Most Advanced Cybersecurity Professionals in the World

Abstract:

It is no secret that the Israelis have surpassed the rest of the world with some of the most advanced cyber capabilities. Several years ago, Dr. Murray attended an event and met a former intelligence officer from Mossad's military intelligence Unit 8200, who described how they began developing alternative methods to identify, assess and recruit new candidates into their service.

The presenter will provide a background on Unit 8200, their mission and discuss some of their more known activities. The discussion will venture into to the assessment and recruitment process which is producing some of the most highly offensive technical operators today, as well as the implications of their skill sets once they leave government service.

Presenter: ***Dr. Shawn Murray***

Shawn Murray is President and CAO at Murray Security Services and was previously assigned to the United States Missile Defense Agency as a Senior cybersecurity Professional. His previous assignments include work with the US Army Cyber Command in Europe, US Air Force and with Commercial Industry in various roles in Information Assurance and cybersecurity. He has traveled the globe performing physical and cybersecurity assessments on critical national defense and coalition programs and has prepared reports for the House Armed Services Committee and has testified on cybersecurity and privacy issues for leaders in Congress. He is the lead cyber consultant at the Pikes Peak Small Business Development Center (SBDC) and sits on the national SBDC cyber working group.

Dr. Murray has worked with SBA, Colorado Attorney General's office, NSA, FBI, CIA and the US Defense and State Departments on various Cyber initiatives and has over 20 years of IT, communications and cybersecurity experience. He has presented as a featured or keynote speaker for numerous conferences across the globe and enjoys teaching and presenting as a guest lecturer on Cybersecurity, business and computer science courses at his Cyber Academy and for several universities. He has several industry recognized certifications to include the C|CISO, CISSP and CRISC. He holds several degrees to include an Applied Doctorate in Computer Science with a concentration in Enterprise Information Systems.

Dr. Murray is a distinguished fellow at the Information Systems Security Association and a past president of their International Board of Directors. He enjoys spending time traveling with his family, researching and collaborating with other professionals in cybersecurity and Cyber Law and plays soccer in a local league in Colorado Springs.

AI in Critical Infrastructure: Ethical and Security Challenges

Abstract

AI is rapidly transforming critical infrastructure sectors like energy, healthcare, and finance, driving efficiency and automation at unprecedented levels. However, this rapid adoption exposes ethical risks, security vulnerabilities, and regulatory gaps that could have catastrophic real-world consequences. This presentation introduces the RISE (Research, Implement, Sustain, Evaluate) and CARE (Create, Adapt, Run, Evolve) frameworks, two complementary strategy and governance models designed to operationalize AI strategy and security. Attendees will gain a structured approach to embedding AI governance, risk management, and compliance into AI-driven critical infrastructure projects, ensuring AI systems are ethical, secure, and resilient against adversarial threats. Through examples and a governance-first perspective, this session will equip security leaders with actionable strategies to mitigate AI risks in high-stakes environments where failure is not an option.

Presenter: ***Rock Lambros***

Kyriakos "Rock" Lambros is a leader in business-aligned AI and cybersecurity. As CEO of RockCyber, he leverages over 20 years of expertise to develop security solutions across sectors like energy, eCommerce, and banking. He has minimized risks at corporations like MPLX, eBay, and General Dynamics.

He holds an MBA from Arizona State University and a B.S. in Management Information Systems from the University of Nevada, Las Vegas. As co-author of "The CISO Evolution," he integrates cybersecurity into business strategy. Active in ISSA and several OWASP AI initiatives, his insights help companies navigate modern cybersecurity and AI complexities.

Building a Home Lab in the Cloud with AWS and CloudGoat

Abstract:

This presentation explores the creation and utilization of a cloud-based home lab, leveraging RhinoLab's CloudGoat. This vulnerable-by-design AWS environment, developed by Rhino Labs, provides a hands-on experience for security enthusiasts to enhance their skills in cloud security. With the increasing migration of infrastructure to cloud environments, especially in the government sector, this presentation highlights the importance of gaining practical knowledge in this field.

Key topics covered include the benefits of using AWS for a low-cost or no-cost home lab, the importance of hands-on experience with various operating systems, and precautions to take when using AWS free tier resources. Additionally, the presentation delves into CloudGoat's setup process, its features, and the resources available for users, such as GitHub repositories and tutorial videos.

Presenter: ***Eric Crump***

Eric Crump is a Cybersecurity Engineer currently working for HDS CISA. A retired veteran Eric's background in Chemical Defense, Intelligence analytics, and logistics have helped solidify his ability to support the United States in securing our national critical infrastructure. Eric also volunteers with supporting transitioning service members, or recent graduates, navigate the hiring process and secure positions to support the United States in Cybersecurity.

Social Engineering, Past and Present

Abstract:

Social engineering is the art and science of using psychological factors to manipulate or deceive a targeted victim in order to gain control over a computer system; or to steal critical or coveted information, be that personal, business, or financial information. All social engineering attacks are generally the utilization and leveraging of six psychological principles. With the surge of artificial intelligence (AI), hackers are doing the same thing everyone else is doing, ….. using AI to automate tasks, solve complex problems, analyze massive amounts of data, and improve efficiency, but in social engineering. This presentation will walk through how the past (psychological factors) meets the present (AI).

Presenter: Stan Richister

Stan "Stanimal" Richister has over 30 years of military and corporate experience in leadership and management as a United States Air Force Cyber Warfare Officer, Network Operations Officer, and Air Operations Staff Officer, working in or with the National Security Agency (NSA), National Reconnaissance Office (NRO), Federal Bureau of Investigations (FBI), Department of Homeland Security (DHS), Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), Air Combat Command (ACC), Air Force Space Command (AFSPC), United States Forces Korea (USFK), North American Aerospace Defense Command - Northern Command (NORAD - NORTHCOM), Special Operations Command (SOCOM), and Joint Special Operations Command (JSOC) in Offensive and Defensive Cyberspace Operations, Network Operations, Information Operations, Cyber Intelligence, Tactical Air Operations, Space Operations, Missile Defense and Missile Warning Operations,

Mobility / Logistics, and Joint Electromagnetic Spectrum Operations (JEMSO). He has commanded three Cyber Flights, and served as a Cyber Warfare Squadron Assistant Director of Operations (ADO), a Network Operations Squadron Director of Operations (DO), squadron and combat operations group executive officer, Air Staff and Combatant Command Action Officer and Cyber Branch Chief, a Numbered Air Force Cyber Division Chief, and Air Force Space Command Cyber Division Chief. In JSOC, he was an Operations Officer and Flight Commander, ensuring the execution of Cyber enabled Special Operations on High Value Targets (HVTs).

He is a Certified Air Force Instructor ("K-Prefix") and was also qualified in an Air Force Cyber Weapon System.

Stanimal retired from Special Operations Command, as the Chief, J-3 Cyber Operations, Space Operations, and Joint Electromagnetic Spectrum Operations; where he was the first and only person in DoD coordinating and integrating Cyber, Space, and Electromagnetic Warfare Operations and capabilities in Special Operations and across Special Operations Forces for Homeland Defense.

He received his undergraduate degree in Geography from the University of South Carolina and Master's Degree in Telecommunications Management from the University of Maryland University College, now the University of Maryland Global Campus (NSA / DHS National Center of Academic Excellence), as well as had education and training at the NSA National Cryptologic University. He is a graduate of the Air War College; the Joint Forces Staff College Information Operations Division; Army Information Operations Capabilities, Applications, and Planning Course, and Military Deception Planners Course. He is a Certified | Chief Information Security Officer (C|CISO) and holds a Federal Aviation Administration Private Pilot Certificate.

He is a member of the:

- Information Systems Security Association - Colorado Springs (ISSA - COS)

- International Information Systems Security Certification Consortium (ISC2) - Pikes Peak Region

- Military Cyber Professionals Association (MCPA) - Colorado Springs Chapter

- Association of Old Crows (AOC) - Pikes Peak Roost (Colorado Springs)

- Open Worldwide Application Security Project (OWASP) - Colorado Springs Chapter

- Veterans of Foreign Wars (VFW), Post 101

Stanimal is a sought out dynamic public speaker, advisor, consultant, and mentor on full spectrum Cyberspace and Information Operations, as well as Air, Space, Special, and Missile Defense and Warning Operations. He is a tactical aviation junkie and a musician, playing five instruments, and enjoys writing and recording his own songs in his home recording studio.

CFW Emcee

Halie Anthony

Halie Anthony brings over 20 years of IT experience across multiple industries to include DoD, Healthcare, and Education. She holds a bachelor's degree in business administration and management and an MBA from Colorado Technical University along with numerous technical and industry certifications.

In the healthcare industry, Halie previously served as the Operations Manager for Clinical Engineering and was promoted into a health system manager role over the Ancillary Applications department at the University of Colorado Health System. Her teams were responsible for medical device management within the Colorado Springs hospitals as well as the software applications that interfaced with those devices across the entire front range. Her teams helped deploy the Mobile Stroke Unit, took on telehealth projects, and led the initiative of securing medical devices with cyber vulnerabilities.

Halie is an adjunct professor and lead instructor for The College of Biomedical Equipment Technology and Charter College. Her engaging (and entertaining) classes are focused on IT fundamentals, leadership development, and cybersecurity.

Halie currently works as a director for Leidos and serves as the IT Enterprise Operations Manager for NASA. Her unique ability to blend IT, medical device management, and cybersecurity along with her passion for teaching make her a valuable addition to our team.

Cyber Focus Week

ISSA
Information Systems Security Association
Colorado Springs Chapter

CFW Sponsors

RISE Executive Coaching
Elevate Your Leadership

LAVERTY CYBER

CLEARED CAREERS

CFW Presenting Partners

PIKES PEAK
REGION