23rd Annual UNC Charlotte Cybersecurity Symposium

Presented On Campus // October 12-13, 2022

Presented by: BANK OF AMERICA

In Collaboration with ISSA Charlotte Information Systems Security Association

Wed Oct 12 2022

8:00-8:50 Continental Breakfast, Exhibition opens (Lucas Ballroom)
8:50-9:00 Welcome (McKnight Auditorium)
9:00-10:15 Opening keynotes

- *The Nexus of Cyber Security and Fraud: Combating Cybercrime*David Nardoni, Bank of America
- *Fragilience Redux: Why Cyber Resilience is a sham, Fragility is the norm, and there is no discipline to our discipline* Christofer Hoff, LastPass
- *New Paradigms for the Next Era of Security (DIE Triad)*Sounil Yu JupitorOne

10:15-10:45 Break (Lucas Ballroom)
10:45-11:30 Breakout sessions

- *Automating Insecurity in Azure* Karl Fosaaen, Netspi (Cone 210)
- *Panel: API and Microservice Security* Brian White Wells Fargo, John Melton Oracle, Oz Golan Noname Security (Cone 112)
- *Defending Against New Phishing Attacks That Abuse OAuth Authorization Flows* Ray Canzanese, Netskope (Cone McKnight)
- *Panel: Third Party Risk:* Doug Rambo Ally, Bob Maley Black Kite, Michael Thelander eclypsium, Patrick T Audet Ally (Library Halton Reading Room)
- *Mainframe Application Security* Jay Smith Wells Fargo, Jan Nunez Wells Fargo (Cone 111)

11:30-11:45 Break (Lucas Ballroom)
11:45-12:30 Breakout sessions

- *Panel: Cloud SOC* Rick Doten Centen, Todd Inskeep Inovate Solutions, Ben Anger Unum Group (Cone 112)
- *Planning for PCI v4.0 - How a merchant stays on top of the ever changing data security landscape*Jacqueline Volkmann Black Lowes (Cone 210)
- *Enhancing SecOp Practices with MITRE* Chris Boehm SentinelOne (Cone McKnight)

- *Deconstructing Zero Trust* Vinicius Da Costa, Bank of America (Cone 111)
- *Panel: Incident Response* Brent Biglow Charlotte ISSA, Jefferson Pike Lowes, John Riddlemoser TIAA (Library Halton Reading Room)

12:30-1:30 Lunch (Student activity center)
1:30-2:15 Coffee, Dessert, networking, and drawings (Lucas Ballroom)
2:15-3:00 Breakout sessions

- *What's Lurking in Your Network?* Kurt Wassersug Sepio (Cone 210)
- *Panel: Cybersecurity Career Paths* Jackie Volkmann Black Lowes, Jared Heintz TIAA, Ben Anger Unum Group(Cone 112)
- *Panel: What's New in Cybersecurity Law?* Allen O'Rourke Truist, Michael Parello Ally, Kamal Ghali Bondurant Mixson & Elmore LLP (Library Halton Reading Room)
- *Cybersecurity Insurance: Where to Start & How to Qualify* Christopher Hill, Beyondtrust (Cone 111)
- *Trusting and Defending Risk Measurements* Jack Jones, FAIR Institute (Cone McKnight)

3:00-3:15 Break (Lucas Ballroom)
3:15-4:00 Breakout sessions

- *Panel: Post Quantum Security* Sam Phillips Wells Fargo, Yongge Wang UNC Charlotte (Cone 112)
- *Panel: Ransomware: A Year in Review* Chris Furtick Fortalice Solutions, Katherine Wise FBI, Rick Scott Bank of America, Joe Schottman Security Researcher (Library Halton Reading Room)
- *Protecting Cyber-physical Systems* Russell Richardson Duke Energy (Cone McKnight)
- *Panel: Diversity in Cybersecurity Workforce* Matt Donato Cybersn, Christina Bray Collins Aerospace, Tammy Moskites CyAlliance (Cone 111)
- *The 3 Ways of DevOps as the Keys to Developer-Centric Application Security*Larry Maccherone Contrast Security (Cone 210)

4:00-4:15 Break (Lucas Ballroom)
4:15-5:00 Keynote session

- **CISO Panel** (Cone McKnight)
  - Todd Inskeep Inovate Solutions
  - Donna Hart Ally
  - Howard Whyte Truist
  - Noah Davis Trane

Thursday Oct 13 2022

8:30 Registration and Coffee (Student Activity Center Solons)
9:00-12:00 Workshops
12:00-1:00 Lunch
1:00-4:30 Workshops

THREATOPS Challenge (CTF): 1:00-3:00 *SentinelOne.* (attendees can participate virtually) **Student Activity Center D-E**
Join your fellow cybersecurity peers for our ThreatOps Challenge, which will incorporate both known and advanced persistent threat attack vectors and methodology. You must register to participate.

Workshop (9:00-12:30) Student Activity Center Salon D-E

Benjamin Agner - UNUM
Bio: Benjamin (Ben) Agner is an experienced IT and security leader, engineer, consultant, architect, and public speaker. He has an extensive track record of delivering secure digital transformation and innovation at scale through cloud enablement, zero trust security architectures, and modern (Agile/DevSecOps) team structures.

Professionally, Ben currently serves as the Global Deputy CISO and Head of Security Solutions Engineering at Unum, where he leads the Security Assurance, Security Solutions Engineering, and Governance, Risk, and Compliance functions globally. He also serves as the Security/GRC Lead for the Rocky Enterprise Software Foundation (RESF), which builds and maintains one of the most popular open-source enterprise Linux operating systems, Rocky Linux.

Prior to Unum, he served as the Director of Global Security Portfolio Management at Aflac, where his responsibilities included the management and modernization of the Global Security portfolio of services, the delivery of all M&A security activities, and serving as the security lead for the company's vertically integrated portfolio companies in the US. He also served as the head of IT security and compliance at Empowered, a SaaS-based benefits management startup that was acquired by Aflac, where he was instrumental in securely scaling the company's benefits enrollment platform from 50,000 to 15 million users and $1.5 Billion in annual revenue in under two years. Prior to that, he has more than 10 years of experience as a cyber security consultant, lead systems engineer, Big 4 compliance auditor and startup entrepreneur.

Patrick Audet - Ally
Bio: Pat started his technology career over 30 years ago focusing on technology and infrastructure. Based in the Detroit area, Pat supported manufacturing with time at Ford, EDS, Detroit Diesel and R. L. Polk. Pat joined Ally over 7 years ago and leads the Third Party Cyber Risk team. When not at work Pat can be found outdoors travelling and Mt biking.

Jackie Volkman Black - Lowe's
Bio: Jackie Volkmann Black is a Director of Information Security at Lowe's where she leads the Security Compliance team. In her role, she is responsible for the global compliance for Payments (PCI), other regulations and frameworks (SOX, HIPAA, GLBA, CTPAT, etc.), Asset Management for Security, and Data Protection teams for the enterprise. She joined Lowe's in 2010 where she started in the Internal Audit department identifying operational and technology process improvements . In 2015, Jackie took on responsibility of PCI Compliance and played an important role in transforming Lowe's PCI environment. She later moved into Information Security to stand-up and mature the risk and compliance functions. Jackie participates in the Lowe's Women in Tech resource group where their mission is to connect, inspire, grow, and empower women across technology to lead organizations and build products that reflect the diversity of Lowe's. Jackie has earned a Bachelor of Business Administration in Management Information Systems. She is also a Certified Information Security Auditor (CISA) and Internal Security Assessor (ISA). Jackie spends her free time with her husband, dogs, and family and friends. If Jackie is not at home, she is traveling someplace new and hopefully adding another stamp to her passport.

Chris Boehm - SentinelOne
Bio: Chris Boehm currently works as Technology Strategist at SentinelOne. As a cybersecurity thought leader, he drives strategy and works closely with some of the

largest organizations in the world. Prior to SentinelOne, he was a Senior Product Manager at Microsoft in the Azure Security engineering division. In his 5 years at Microsoft, he focused on driving product strategy and delivering strategic customer enablement. Chris worked closely with the Microsoft Cyber Defense Operations Center (CDOC) and Microsoft Threat Intelligence team (MSTIC) to work side by side on research and enablement to create a more intuitive investigation experience for Security Operations Centers.

Christina Bray - Collins Aerospace
Bio: Christina Bray is currently serving as Deputy CISO at Collins Aerospace, a subsidiary of Raytheon Technologies living and working in North Carolina's Piedmont area. She is an experienced Information Security and Risk Executive with a focus on building and maturing information security and risk programs for billion dollar industry leaders. Christina's business acumen, approachability and consultative approach improves risk management at every level of the enterprise. As a servant leader, translator, communicator and systems security advocate, she creates a strong cybersecurity culture and improves decision making by advising senior leadership teams on risk potential. Her 20+ years of technology and risk experience extends across Aerospace, Financial Services, Professional Services, Consulting, Insurance, Transportation and Logistics industries.

Doug Britton - Venture Backed Companies
Bio: Doug is an experienced and accomplished entrepreneur, having started four B2B-focused, venture-backed companies. Doug focuses on working with inventors, pre-company formation, to make sure the precursors for a successful organization are in place. Doug's ventures have been in cybersecurity and aviation. His businesses have raised more than $10m from name-brand VCs like Bessemer Venture Partners and Lockheed Martin. He has overseen innovative IP management in each of the companies, securing nine US patents as an inventor and shaping nearly 30 patents from inventors on his time. He sold his first company to Samsung.

Prior to starting his first company, Doug was an R&D manager in cybersecurity at Lockheed Martin. During his 9 years at Lockheed, Doug focused on classified programs in cybersecurity and IT management. Before that, Doug was a Russian linguist in the US Army's 10th Special Forces Group.

Ray Canzanese - Netskope Threat Labs
Bio: Ray is the Director of Netskope Threat Labs, which specializes in cloud-focused threat research. His background is in software anti-tamper, malware detection and classification, cloud security, sequential detection, and machine learning. He holds a Ph.D. in Electrical Engineering from Drexel University. Most recently, Ray was the CTO of cloud security startup Sift Security.

Expertise: behavioral malware analysis, machine learning, data mining, data and decision fusion, sequential detection, graph analytics, honeypots, AWS, Windows OS Internals

Vinicius Da Costa - Bank of America
Title: Deconstructing Zero Trust

Bio: In his role as a senior vice president at Bank of America, Vinicius Da Costa is responsible for delivering zero trust architecture, a strategic approach to cyber security that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction. He is an information technology and security professional with 25 years of experience in the financial services, retail and consumer goods industries.

An advocate of diversity and inclusion, Vinicius is involved with the nonprofit Citizen Schools, which helps enhance the education of children in low-income communities. He is also the Chairperson of the Hispanic Information Technology Executive Council Foundation (HITEC) internship program and was a board member at Association of Latino Professionals for America Charlotte (ALPFA).

Vinicius holds a Master of Information and Cybersecurity degree from UC Berkeley and is fluent in Portuguese, English and Spanish. He resides in Charlotte with his wife, three kids and two dogs.

During another year of record cyber-attacks, companies and cybersecurity professionals are still struggling with how to implement Zero Trust Architecture and reap its benefits. In this session we will break down the main domains involved in securing an institution’s environment (User, Device, Network, Data, Application) and share a simplified set of actions that can accelerate a Zero Trust program and prepare cybersecurity professionals.

Noah Davis - Trane Technologies
Bio: Noah Davis is an internationally experienced risk driven security executive qualified by progressive achievement in IT compliance, cybersecurity, and operations within Fortune 500 diversified manufacturing organizations. He has established himself as highly successful at partnering IT with business, streamlining operations, and taking a risk based approach to optimize cost. He brings over 20 years of experience with senior leadership roles across security domains covering incident response, controls, architecture, access, data, endpoint, identity, and network.

Matt Donato - CyberSN
Bio: Matt Donato is the managing director of growth strategy and partnerships at CyberSN, the largest cybersecurity talent acquisition technology and services firm in the U.S.. He is an accomplished business leader and strategic advisor in the fields of cybersecurity, professional services, staffing solutions and executive search.

Matt’s career spans approximately 20 years with experience in professional recruiting, talent management, strategic consulting, and staffing experience in all facets within the cybersecurity industry, as well as staffing in the security, risk management technology, finance, operations, and engineering sectors. Over the years, Matt has focused on value creation, integrating sales and marketing, and recruitment strategies into the overall business strategy of an organization to help protect companies and provide the solid foundation they need to grow and transform. He has led the conversation on talent acquisition and development, large-scale sales and operations providing insight on the existing landscape in cybersecurity.

Rick Doten - Centene

Bio: Rick Doten is VP, Information Security at Centene Corporation, and CISO of Carolina Complete Health based in Charlotte, NC. Rick supports both the NC health plan and corporate Centene in a cybersecurity leadership role.

Among recent accomplishments, Rick worked as Virtual CISO supporting international companies, including developing and maturing the IT security program at a large Mexican conglomerate, international datacenter provider, and US sports league. Rick also developed the curriculum for a Cybersecurity Master's degree program for Monterrey Tech University.

Rick has been cited in industry publications and on television commenting on issues relating to cybersecurity and risk management. He is a member of The CyberWire Hashtable, and on the editorial panel for the Council on Cybersecurity 20 Critical Security Controls, currently working on updating version 8 of the controls.

Rick ran ethical hacking, incident response and forensics, and risk management teams throughout his 25-year cybersecurity career. Previously, Rick was cybersecurity practice lead for an intelligence and security firm Crumpton Group, was CISO of DMI, a multi-national US company, and has held positions as a Risk Management consultant at Gartner, Chief Scientist for Lockheed Martin's Center for Cyber Security Innovation, and Managing Principal in the Professional Security Services practice at Verizon.

Dan Dunkin - AT-NET Services
Bio: Dan Dunkin is Chief Engineer and CTO of AT-NET Services, a Premier Cybersecurity Managed Services Provider headquartered in Charlotte, North Carolina and serving the southeast.

Dan has assisted businesses with their technology needs for over 38 years. Combining a background in technical engineering and business ownership, he is skilled at designing technical solutions to business problems. As a member of the AT-NET team, Dan creates implementation procedures to help clients get the most value from their investment in technology. He is responsible for overseeing all aspects of technology at AT-NET.

Prior to joining AT-NET, Dan held positions as a control systems engineer for TRW Electronics and Defense and as the owner of Advanced Systems Group, a systems integration firm providing network design, system security, and custom applications for clients ranging from small businesses to Fortune 100 giants.

Dan graduated from Purdue University with a degree in Aerospace Engineering and performed post-graduate study in Flight Dynamics at UCLA.

When not working, Dan likes to play basketball and coach recreational football, soccer, basketball, and baseball.

Desirée M. Ericksen - Internetwork Engineering
Bio: Desirée M. Ericksen, CISSP, is a Security and Compliance Consultant with Internetwork Engineering. In her role, she has worked with various organizations to assist in developing and strengthening security posture through assessing risk, policy and procedure creation, and consulting services.

From developing and implementing a Third-Party Risk Management Program in a financial institution to assisting clients throughout the country with their Third-Party Risk Management needs, she draws on more than 18 years' experience in Third-Party Risk Management.

Desirée, a mother of three and Tutu of one, lives in Swansboro with her youngest, Madison. Her son, Alex, lives in Raleigh and is attending Wake Technical Community College. Her daughter Hannah, son-in-law Chris, and grandson Grayson, live in Apex. Desirée spends her free time refinishing furniture, designing, and building custom pieces.

Jeremiah Fellows - Bank of America
Title: "Engineering Human Experiences – Designing Simple Solutions in Today's Complex Environments"

Bio: Jeremiah has been a neurophysiology researcher, an IT manager and a jet-setting sales and marketing guy. He has inspected factories in Xi'an, negotiated deals in Guadalajara, and lectured in Bogotá. Jeremiah has branded companies, products, services and cattle.

These diverse experiences have always been tied together by the question: How can we better serve the people who build, buy, support, and maintain our products and services? This question led Jeremiah to Service Design. Now a Senior service designer with the employee experience design (EXD) team, Jeremiah is passionate about using design thinking, user research, and service design to craft effective, efficient, and enjoyable experiences. He is a frequent writer and speaker on topics at the intersection of design, technology, and culture.

Abstract: Problems never exist in a vacuum, but many times problems are discussed in a silo. This often leads to solutions that consist of additional layers of technology and processes. We are not taking the time purposefully looking at a slice of the whole ecosystem from the user's perspective and peeling back layer by layer to examine how each layer, people, processes, and technologies contribute to the problem. As a result, we create increasingly more complex processes, systems, and products. When teams take a user-centric, systems wide approach to identifying and solving problems, the opportunity for simplification becomes evident. Solution by subtraction can lead to better user experiences, more scalable and extensible technologies, and processes that support the needs of the business AND the users. Come and join us in a discussion of how the intersection of UX Researchers, UI Designers, and Developers design and create human experiences that reduce complexity and drive innovation.

Karl Fosaaen- NetSPI
Bio: As a Senior Director at NetSPI, Karl leads the Cloud Penetration Testing service line and oversees NetSPI's Portland, OR office. Karl holds a BS in Computer Science from the University of Minnesota and is approaching 15 years of consulting experience in the security industry. Karl spends most of his research time focusing on Azure security and contributing to the NetSPI blog. As part of this research, Karl created the MicroBurst toolkit (https://github.com/Netspi/Microburst) to house many of the PowerShell tools that he uses for testing Azure. In 2021, Karl co-authored the book 'Penetration Testing Azure for Ethical Hackers' with David Okeyode. Over the years, Karl has held the Security+, CISSP, and GXPN certifications. Since DEF CON 19, Karl has spent most of his conference time selling merchandise as a Goon on the Merch (formerly SWAG) team.

Chris Furtick - Fortalice Solutions
Bio: Chris Furtick is a proven information security leader and vCISO with a consultative voice able to bridge the gap between technology and business outcomes. A technically proficient professional, he has experience advising C-level executives and technical engineers in fundamental and advanced information security tactics and strategies. He is a passionate leader accomplished in interpreting business objectives and motivating team members to measure success and meet business requirements.

As Director of Security Engineering & Incident Response for Fortalice Solutions, Furtick manages a team of incident responders and security engineers; leads all incident response and planning activities for Fortalice clients; performs incident triage from a forensic perspective, including determination of scope, urgency, and potential impact; acquires or collect computer artifacts, including malware, user activity, and log files; and provides threat analyses mitigation/countermeasure recommendations, after action reports, summaries, and other situational awareness information in areas such as perimeter defense; malicious software analysis; attack vector analysis; computer network defense; incident handling; risk analysis and readiness; and strategic planning analysis.

Prior to joining Fortalice, Furtick worked as Director of Security Engineering for NorthState Technology Solutions where he served as the primary leader of two security engineering teams, Security Tool Implementation and Staff Augmentations, managed multiple projects valued at $3.6M per year and gained consulting experience in the following sectors: banking/financial, retail, healthcare, manufacturing, energy, education, government, military, insurance, legal, and telecom.

Furtick earned a Bachelor of Science in Computer Science from Southern Wesleyan University as well as multiple certificates, including CISSP Certified Information Systems Security Professional (ISC)², GPEN GIAC Certified Penetration Tester, GSLC GIAC Security Leadership Certification, GCCC GIAC Certified Critical Security Controls Certified Professional, GCPM GIAC Certified Project Manager, GLEG GIAC Certified Law of Data Security Certified Professional and CDE CyberArk Certified Delivery Engineer. He served as Technical Editor for the McGraw-Hill publication, “GPEN All-in-One Guide” as well as Security Leadership Subject Matter Expert for SANS. He is affiliated with multiple professional organizations including FBI InfraGard, ISACA, PMI, SANS Advisory Board.

Kamal Ghali - Bondurant Mixson & Elmore LLP
Bio: Kamal Ghali is a partner at Bondurant and a top-ranked trial lawyer recognized in “Best Lawyers in America” and “Chambers USA: America’s Leading Lawyers for Business.”

A former federal prosecutor, Mr. Ghali has handled some of the biggest civil and criminal cases in the country including billion-dollar commercial disputes, complex criminal fraud investigations and prosecutions, and high-profile international cybercrime investigations involving numerous international targets. He has deep experience in high-stakes business litigation, often involving fraud and data security issues; government investigations and white-collar criminal cases; and a range of cybersecurity matters. He’s received numerous commendations from the U.S. Department of Justice, including a Director’s Award for “superior performance” in co-prosecuting the promoters and developers of SpyEye, a notorious malware that inflicted nearly a billion dollars in losses worldwide. Before returning to Bondurant, he served as a U.S. Department of Justice white-collar and cybercrime prosecutor for over six years, including as a deputy chief at the U.S. Attorney’s Office in Atlanta. He leads Bondurant’s Cyber & Digital Litigation Practices.

Oz Golan - Noname Security
Bio: Oz Golan is the Co-founder and CEO of Noname Security, the first API Security unicorn startup which was founded in 2020. Previously Oz held multiple leadership positions including Research Team Lead and Director of R&D in the Israeli cybersecurity sector. Before his civilian career, he spent 5 years as a Security Researcher and Developer in Unit 8200 of the Israeli Intelligence Corps. Oz holds a Bachelor of Science in Physics and Computer Science from The Hebrew University of Jerusalem and is currently based in Tel Aviv, Israel.

Donna Hart - Ally Financial
Bio: Donna has 25 years of technology experience. Her career began as an associate with First Union and worked in several areas including Technology Program Office, Desktop Services, several roles within Network Services, Technology Production Operations, and Information Security . She joined Ally as the Chief Information Security Officer on Feb 1st, 2021 from Wells Fargo Corporation. In her spare time she enjoys hiking, attending her son's sporting events and loves to volunteer for Animal Charities.

Jared Heintz - TIAA
Bio: Jared Heintz retired from active-duty service in 2018 after serving just over 20 years. Jared retired as a Chief Warrant Officer in cybersecurity, with experience in cyber risk and governance, compliance, blue teaming, red teaming, and security operations. After military retirement, Jared joined TIAA as the Senior Manager of Global Cybersecurity Operations, managing a large team of cyber security analysts on the continuous defense of TIAA networks and applications. Jared has just over 25 years of experience in IT and cybersecurity. He serves as a subject matter expert with ISC², where he helps to develop new exam questions for the CISSP.

As an advocate for diversity and inclusion, Jared serves as one of two national co-chairs for the Our Corps veterans resource group, which helps to advocate for veteran inclusion and awareness within the workplace at TIAA. He also serves as a life member of the Military Officer's Association of America and the Vice President of Retired Affairs for the Coast Guard Chief Warrant and Warrant Officer's Association.

Jared holds a Bachelor of Arts in Intelligence Studies from American Military University and is completing his Master of Business Administration later this year. He resides in Charlotte with his wife, four kids, a dog, and a cat.

Jon Hightower - GreerWalker LLP
Bio: Jon joined GreerWalker LLP in 2018 as Director and is the firm's knowledge leader in IT Risk. Prior to joining the firm, Jon was the director of Information Security and Compliance for the largest privately owned retail company in the nation. In addition, Jon has 11 years experience in Public Accounting where he provided IT Risk and Assurance Services to companies ranging in sizes from small to mid-market, to companies in the Fortune 500.

Jon focuses on providing practical, high value solutions that achieve the goals of reducing IT risk for his clients. His extensive experience in multiple industries as well as his technical understanding of risk has provided him with invaluable insights in navigating the complex world of Cloud, IoT, Cybersecurity, Data Privacy, and Compliance.

Christopher L. Hills - BeyondTrust

Bio: Christopher L. Hills has more than 20 years' experience as a Technical Director, Senior Solutions Architect, and Security Engineer operating in highly sensitive environments. Chris is a military veteran of the United States Navy and started with BeyondTrust after his most recent role leading a Privileged Access Management (PAM) team as a Technical Director within a Fortune 500 organization. In his current position, he has responsibilities as a Chief Security Strategist (America's) working with Customer, Marketing, and Executives on Thought Leadership, Market Trends, Company Vision and Strategy reporting to the CSO. Chris has held the Deputy CTO and Deputy CISO role since starting with BeyondTrust. Chris is also co-author in the recently released Cloud Attack Vectors book. In his free time, Chris enjoys spending time with his family on the water boating, supporting his son's football career as a senior, going to the sand dunes and offroading.

Christofer Hoff - LastPass

Title: Fragilience Redux: Why Cyber Resilience is a sham, Fragility is the norm, and there is no discipline to our discipline

Bio: Christofer Hoff is Chief Secure Technology Officer of LastPasss. Before joining LastPass, Christofer had multiple cybersecurity leadership roles at Bank of America. Prior to working at Bank of America, his roles include the Chief Information Security Officer at Citadel, Vice President and Security CTO at Juniper Networks, and Director of Cloud & Virtualization Solutions at Cisco Systems, among other security-focused roles.

In addition to his professional leadership responsibilities, Chris takes an active role in engaging youth in the impact of technology, privacy and security on society and culture as founder of HacKid, an interactive STEAM conference for parents and kids from diverse backgrounds. Chris was a founding member of and technical advisor to the Cloud Security Alliance and serves as an advisor to numerous companies and organizations.

Abstract: We shall explore that from a Cyber Security perspective, instead of hand-waving about the virtues of resilience, we should instead focus on anti-fragility.

Cyber Security is a quality problem, which in turn represents a safety problem, and we haven't evolved to think about what's needed to solve anything more than hygiene basics and our definition of "winning" is simply "not losing." We have more gadgets than we know what to do with. We don't need more sensors or sense-making systems. Instead, the reason we are largely fragile and things don't get better, is that we don't take the time to define or invest in decision systems to actually make risk-based decisions.

Here's how you can start...

Todd Inskeep - Innovate Solutions
Bio: Todd Inskeep brings 30 years of executive leadership and innovation experience to delivering business results and managing cybersecurity risk. He has been Chief Information Security Officer, lead wide-ranging cybersecurity projects for global and regional companies, and worked in multiple industries including financial services, intelligence, pharmaceuticals, and manufacturing. He's built and managed cybersecurity teams and budgets to reduce cyber risk. An accomplished speaker and writer, Todd holds multiple patents and was Bank of America's Executive-in-Residence at the MIT Media Lab. Todd started working product and software security at the National Security Agency and holds both a BSEE and a Master of Science in Strategic Intelligence. Active in the infosec community, Todd is on the RSA Conference Advisory Board and has been on the Program Committee for many years. Todd currently runs Incovate Solutions LLC, a consulting company focused on building world-class cybersecurity leaders and programs.

Jack Jones - FAIR Institute
Bio: Jack has worked in information security for over thirty-five years, ten years of which as a CISO with three different companies, including a Fortune 100 company. His work was recognized in 2006 with the ISSA Excellence in the Field of Security Practices award. In 2012 Jack received the CSO Compass award for risk management leadership. Jack also had the privilege of being on the ISACA task force that created the original RiskIT framework, and he led the development of ISACA's CRISC certification program. An adjunct professor at Carnegie Mellon University, he teaches in the CRO and CISO executive programs. Jack also created the "Factor Analysis of Information Risk" (FAIR) model which has been adopted as an international standard. Currently, Jack is the Chief Risk Scientist at RiskLens and Chairman of the FAIR Institute, an award-winning global non-profit organization with over 13,000 members worldwide. He has also co-authored a book on FAIR entitled "Measuring and Managing Information Risk, a FAIR Approach" which was inducted into the Cyber Security Canon in 2016.

Ray Kelly - Synopsys
Bio: Ray Kelly is an internet security professional with over twenty five years of development experience, twenty of which has focused on the internet security space. Ray has been a key player in multiple successfully acquired cyber security start-ups. He was the lead developer and business unit director for WebInspect with SPI Dynamics which is an industry leading application security scanner (later HP and Micro Focus). Ray holds three web application scanning patents and speaks regularly at security conferences. Today, Ray is a Fellow at Synopsys (formally WhiteHat) where he contributes to research, sales and vision of the security product line.

Emily Loker - NCFTA
Bio: Emily Loker graduated with a B.A. in Psychology from Penn State and with a M.A. in Psychology from Chatham University. Currently in school for a second master's degree in Applied Intelligence from Mercyhurst University. Works within the ransomware initiative at the NCFTA.

Larry Maccherone - Contrast Security
Title: A Transformation Blueprint for Developer-Centric Application Security

Bio: Larry's work has empowered 600 development teams to take ownership of the security of their software. He embodies a rare combination of deep cybersecurity background with current software development experience. He was a founding Director at Carnegie Mellon's CyLab and co-led the launch of Build-Security-In initiative but is also the author of a dozen or so open source projects, one of which gets a million downloads per month, and all of which utilize the approach he advocates for.

Abstract: NIST, SANS, OWASP, PCI, etc. provide lists of candidate application security practices, but the items in the list are unprioritized, target security specialists, and fail to specify adaptations needed for a developer-first approach. Attempting to shift these practices left without proper consideration of modern development practices and priorities is a recipe for frustration, resistance, and false starts.

You will come out of this workshop with a Transformation Blueprint for accomplishing the cultural shift to developer-centric application security at your organization. The approach is derived from the program that Larry has used to accomplish this shift for over 600 development teams. Since Larry is a developer, writing code every day, his program is perfectly suited to the way development teams really want to work, rather than how security folks assume they work.

Bob Maley - Black Kite
Bio :Bob Maley, Inventor, CISO, Author, Futurist, and OODA Loop fanatic, is the Chief Security Officer at Black Kite, the leader in third-party cyber risk intelligence. Bob has been a leader in security for decades, initially in physical security as a law enforcement officer. He has acquired a broad range of experience and expertise in all areas of security, including third-party security, risk assessment, architecture, design, policy development, deployment, incident response and investigation, and enterprise solution deployments such as intrusion detection, data protection, compliance, and incident reporting and response.

Before joining Black Kite, Bob was the head of PayPal’s Global Third-Party Security & Inspections team, developing the system into a state-of-the-art risk management program.

In a previous role as Chief Information Security Officer for the Commonwealth of Pennsylvania, he led the Pennsylvania Information Security Architecture program to win the 2007 award for outstanding achievement in information technology by the National Association of State Chief Information Officers (NASCIO).

Bob has been named a CSO of the Year finalist for the SC Magazine Awards and was nominated as the Information Security Executive of the Year, North America. Additionally, his team was a finalist in the SC Magazine Awards for Best Security Team. Bob’s certifications include CRISC, CTPRP, OpenFAIR, and CCSK. His expertise has been quoted in numerous articles for Forbes, Politico, Payments.com, StateTech Magazine, SC Magazine, Wall Street Journal, Washington Post, Dark Reading, etc. He has been published in numerous whitepapers, the IEEE Journal, and his first book, What Every Engineer Should Know About Cybersecurity and Digital Forensics, will be released in December.

John Melton - Oracle, NSBGU
Bio: John is currently the Director of Product Security at Oracle, NSBGU. His experience has

involved moving back and forth between the software engineering and security fields, aiming to get them to play nice together.

Tammy Moskites- CyAlliance
Bio: Tammy is the CEO and Founder of CyAlliance. She is a strategic advisor and "Alliance" builder for companies, vendors and startups by leading, building and scaling their security offerings while providing trusted executive advisory services and professional services for companies worldwide. With her 30+ years of technology experience, she is noted by her peers to be a results-driven and passionate executive leader. She is a distinguished career CISO, and she has held many security and technology leadership roles which include; Accenture, Venafi, Time Warner Cable and The Home Depot. She has dedicated her career to guide CISOs worldwide to help defend their organizations from cyber threats and attacks. She is a highly recognized cyber and women in technology social influencer with thousands of followers. Amongst the many things she is involved in, she is a Venture Advisor to YL Ventures, a Distinguished Fellow with the Ponemon Institute and volunteers her time with organizations including ISACA, Australian Information Security Association (AISA), SheLeadsTech and the ISSA. Tammy hosts CISO Networking events globally to allow CISO's to share, network and build local relationships. She has spoken at conferences and cyber kickoffs around the world and has received many accolades in recognition for her work within the security industry. She is an internationally recognized keynote/speaker, not only on security and governance, but also on career building, women in technology and leadership mentoring. She is a diversity champion in the market and with the companies she has worked. Tammy dedicates her personal time as a professional independent leadership and career coach/mentor. Tammy continually provides strategic guidance to other industry-leading security vendors where she is an Executive Company Advisor and CISO community builder to Adaptive Shield, AppViewX, Blue Lava, Grip Security, Raxis, Vectra AI, and previously to RiskIQ, Attivo Networks, Box, Qualys, SecureAuth, and Venafi. #DoWhatYouLove #LoveWhatYouDo–

David Nardoni - Bank of America
Title: The Nexus of Cyber Security and Fraud: Combating Cyber Crime

Bio: In his role as a cyber crime response executive with Bank of America, David Nardoni is responsible for the Global Information Security (GIS) Cyber Crime Response & Disruption team, with a primary focus on the disruption of threat actor criminal activity aimed at bank clients and customers. Team functions include providing investigative support to fraud partners and developing countermeasures to better mitigate threat activity.

David has over 20 years of experience in cybersecurity. Prior to joining Cyber Crime Prevention, David was responsible for Bank of America's vulnerability analysis, assessing and prioritizing vulnerabilities within the bank environment. In addition, David managed the global functions for the insider threat and malware prevention teams. At PwC he led the response to large-scale credit card breaches and cases involving economic espionage. David also worked for General Dynamics AIS as a malware specialist and digital forensics practitioner, conducting investigations of large data breaches. He is a former law enforcement officer with more than 10 years of experience investigating computer-based crimes.

Abstract: Description As the nexus between fraud and cyber crime continues to narrow, this presentation will explore the origins and the future trajectory of both, including the importance of fraud and information security teams partnering together to deny, detect, disrupt and deter threat actors. In addition to such teams collaborating, individuals must also be able to identify and understand the threats that target them in order to create a truly layered defense with proactive prevention tactics at its core.

Jan A Núñez - Wells Fargo
Title: Mainframe Application Security

Bio: Jan Núñez is a senior cyber security researcher on the Dynamic Application Security Testing (DAST) team at Wells Fargo. He began his career exploring an interest in software engineering and eventually found a passion for ethical hacking. He has since specialized in web, mobile, and mainframe application security testing.

Aside from his professional life, Jan enjoys coding, and exploring various forms of martial arts.

Abstract: Mainframe systems continue to drive global economic activity despite the "legacy" label they are often associated with. In fact, mainframes are responsible for business-critical functions across 70 percent of Fortune 500 companies. If you have ever withdrawn cash at an ATM, done your taxes online, or booked a flight for your next holiday, you have likely interacted with a mainframe. As with all business-critical systems, ensuring they are secure is imperative. In this talk, a team of researchers will discuss mainframe application security with a focus on CICS - the mainframe component that makes online transaction processing possible. They will discuss general mainframe concepts and the current state of mainframe application penetration testing, along with challenges and solutions they encountered throughout their research.

Edgar Ortiz - Solution Architect
Bio :Edgar Ortiz spent many years helping customers build out and scale successful API programs to enable digitally connected experiences, back office integration, and Business-to-Business communication (B2B). The drive to deliver on these initiatives often leaves security gaps and leaves organizations with a lack of understanding of risk. Edgar's goal is to help organizations continue to gain value from their API programs by making APIs not only easy to use, but easy to use securely.

Allen O'Rourke - Truist
Bio: Allen O'Rourke leads the Cybersecurity Team in the Technology Group of Truist's Legal Department. They provide legal support to Corporate Cyber Security and advise the enterprise on cyber legal matters. Before joining Truist, Allen chaired the Cybersecurity and Privacy Practice Group of the law firm Robinson Bradshaw. He has advised on cybersecurity law and incident response for a broad range of organizations. In addition, Allen has handled over 50 trials in state and federal court and has led countless investigations. Before private practice, Allen was a cybercrime prosecutor who helped lead the Cyber Unit at the US Attorney's Office in Washington, DC, where he received two Special Achievement Awards for his work to combat cybercrime. He graduated from Harvard Law School and clerked in the Fourth Circuit and Eastern District of Pennsylvania.

Mike Parello - Ally Financial
Bio: Mike is a member of the Corporate & Securities group within Ally's Legal Staff. Mike's team's responsibilities include formulating and communicating legal advice to Ally's Information Protection & Risk Management, Supply Chain, IT/IS Risk Management, Third Party Risk Management, and Compliance functions, including the groups within those functions focused on regulatory compliance, data security and loss prevention, and incident response.

Prior to his current role at Ally, Mike worked for New York Life Insurance Company and Cantor Fitzgerald & Co.

Mike holds a JD from Villanova University School of Law and a BS in Finance from the University of Maryland – College Park.

Regina Peyfuss - Bank of America
Title: "Engineering Human Experiences – Designing Simple Solutions in Today's Complex Environments"

Bio: Regina joined Bank of America over two years ago. She brings experience working on SaaS (software as a service) micro services applications and teaching 7 – 12th graders computer science.

She is the lead software engineer for the IGA (Identity Governance and Administration) UI/UX platform. In close collaboration with the Enterprise UX/UI team she works on developing the IGA framework to provide other teams the ability to develop Micro Frontends (MFe) in a loosely coupled, maintainable, and scalable environment. She and her team maintain the GDS Angular component library, which is used by MFes to achieve cohesiveness, unity, and reduce development time.

In her free time, you can find her exploring the Rocky Mountains or the Pacific Northwest.

Sam Phillips - Wells Fargo
Bio: Sam Phillips is Senior Vice President, Information Security at Wells Fargo, responsible for establishing the enterprise security architecture including providing security architecture strategy and solutions, vendor and product evaluations, architecture consulting and education for all lines of business. Sam has extensive security industry experience in driving strategic business initiatives, educational development programs, and chairing or participating in large-scale projects focused on improving and implementing security at an industry level.

Prior to joining Wells Fargo, Sam served as Vice President and General Manager and Chief Information Security Officer for Samsung Business Services, responsible for building security support services for large global customers and developing the information security program. Sam served as the Chief Security Officer for Blackberry prior to joining Samsung and developed one of the first integrated physical and logical corporate security programs. In this role, he was also responsible for providing global security advisory services to Blackberry's enterprise customers.

An industry veteran, Sam has held senior leadership and consulting roles at Bank of America and The Boeing Company, focusing on technology security and risk. He has been responsible for enterprise information security programs, information security architecture, identity and access management, security policy and standards, compliance and assessments, product and infrastructure security, risk management, and security innovation.

Sam earned a Bachelor of Science degree in computer science from Montana State University and a Master of Science degree in Information Systems Management from Seattle Pacific University. He is a Certified Information Systems Security Professional and a Certified Information Security Manager.

Jefferson Pike - Lowe's Companies, Inc.
Bio: Jefferson leads the Third-Party Risk Management program for Lowe's Companies, Inc. and is also a board member of the Charlotte InfraGard chapter, which is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector for the protection of U.S. Critical Infrastructure.

Prior to joining Lowe's, Jefferson served in the U.S. Navy as well as in several cybersecurity risk management roles with Time Warner Cable, Wells Fargo, and Fortalice Solutions.

Jefferson earned a Master of Science in Cybersecurity and Master of Business Administration from the University of Maryland University College, as well as a Bachelor of Science in Management from Montreat College. He holds several information security-related certifications including CISSP, CISM, CRISC, and CISA.

Doug Rambo - Ally
Bio: Doug has over 15 years of technology experience, with 11 of those in Banking. His career began working in a corporate email platform for an insurance firm, then moved into industrial technology working for Ingersoll Rand, joined Wachovia/Wells Fargo in several roles from mobile Operations/Engineering/Platform Strategy, Mobile and Remote Security Architect. He joined Ally 3+ years ago, and currently is the Director Lead over Business Line Risk Governance that a portion supports Third Parties and Third Party Risk. In his spare time he enjoys coaching baseball/soccer/golf, spending time on the lake boating and fishing, and spending time with my family.

Russell Richardson - Duke Energy and Piedmont Natural Gas
Title: Protecting Cyber-physical Systems

Bio: Russell Richardson is Sr. Manager of OT Cybersecurity for Duke Energy and Piedmont Natural Gas. Duke Energy serves 7.7MM energy customers, 1.6MM gas customers, and owns approximately 51,000 megawatts of generating capacity. Russell also serves as program delivery lead for the IT/OT Cybersecurity Program, bringing cyber monitoring and response to all operational areas of the company. This includes the Natural Gas, Nuclear Generation, Regulated and Renewable Energy, Commercial Renewables, Customer Delivery, and Transmission business units. He previously managed the IT Cybersecurity Architecture team, as well as the Critical Infrastructure & Operations team. Russell was one of 11 people selected for the first cohort of the Operational Technology Defender Fellowship. This highly-selective education program provides OT security managers in the U.S. energy sector the opportunity to increase understanding of cyber strategies and tactics that state and nonstate actors use in targeting U.S. energy infrastructure, and how the U.S. government is positioned to counter these adversarial activities. The OT Defender Fellowship is sponsored by the Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (CESER), and hosted by Idaho National Laboratory with support from Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. Russell holds an M.S. in Technology and Organizational Leadership from Purdue University College of Engineering & Technology, a B.A. from the University of Minnesota, and various certifications.

Abstract: Cyber-physical systems (CPS), from smart grid to autonomous vehicles, control the world around us and are growing in importance, but they also present new threats and risks from multiple adversaries.

The Stuxnet attack in 2010 brought government and public attention to the need to secure cyber-physical systems. Several incidents since then have demonstrated the importance of protecting CPS, especially our national critical infrastructure.

This talk explores cyber-physical system threats, risks, and impacts, both past and future.

Colton Robinson - NCFTA
Bio: Colton Robinson has completed his Bachelor of Arts and Master of Science degrees in Criminology from Saint Vincent College. Past experience includes time as a Juvenile Probation Officer and mental health casemanagement. Colton has since transitioned into the cybersecurity world at the NCFTA about a year ago as an Intelligence Analyst on the Malware and Cyber Threats team.

Rick Scot - Bank of America
Bio: Rick Scot is a member of the Bank of America Global Information Security (GIS) Cyber Crime Prevention International team. He is the lead of the Europol OSINT Task Force and the banks representative on the Ransomware Task Force, as well as a driver of the telecom work centered around combating telecom scams. Rick is a Security Awareness for Everyone (SAFE) facilitator. He sits on the strategic advisory board for the New York University Cyber Fellowship and is a Mastermind mentor and sits on the Deans Advisory Board and Cyber Symposium planning committee at University North Carolina, Charlotte, College of Computing and Informatics, as well as a mentor.

Prior to his role with Cyber Crime Prevention, he was a member of the GIS Workforce Strategy team and prior to that, supported the Cyber Public Policy team and served as Program Manager for the creation and implementation of the Independent Assessment team, where he designed playbooks and remediation processes, along with creating a system of record and the Payment

Card Industry (PCI) governance transformation. He also holds two patents and has 15 patents pending. Before coming to GIS in 2016, Rick spent four years as a Functional Architect within the home loans and servicing transformation, leading the data, document, and imaging work. Since joining the bank in 2002 as a Senior Business Analyst, Rick has held several positions within Mortgage Technology, including supporting online operations, third party operations, internal lead management, and several data transformations including the Countrywide transition.

Rick studied Communications at the University of Southern California.

Jason Smith - Internetwork Engineering

Bio: Jason Smith leads the Advisory Services team at Internetwork Engineering. Jason is a blogger, and a strategic technologist. Jason, in his role as Sr IT Security and Compliance Consultant, has worked with dozens of organizations to find innovative, cost effective solutions to complex technology problems. Jason holds multiple security and compliance certifications and is a trainer for ISACA.

Jason draws on more than twenty years of experience in IT, IT Security, and Compliance to provide a unique insight into challenging business problems. Jason is a graduate of Western Carolina University (BS – Criminal Justice) and East Carolina University (MS – Technology Systems-Information Security).

Jay Smith - Wells Fargo

Bio: Jay Smith is a lead security researcher for the Dynamic Application Security Testing (DAST) team at Wells Fargo where he is responsible for application, mainframe, and Active Directory security. His work primarily involves research and development, performing penetration tests, and incident response. In addition to his work in cyber security, he has a background in systems and network administration

Outside of his work with Wells Fargo he is FBI InfraGard member, a Synack Red Team researcher, and is active in the local hacker community.

Michael Thelander - Eclypsium

Bio:Michael has a 20-year track record steering product management and marketing teams for successful, innovative companies. His articles and interviews have appeared in SC Magazine, Cyber Defense Magazine, ITProfessional, Cyber Security: A Peer Reviewed Journal, and he speaks at industry events like BSides, Gartner's IAM Summit, and RSA. Michael received CISSP training through SANS and has been in the cybersecurity space for over twelve years: before Eclypsium he headed product management at Tripwire, ran product marketing at digital fingerprinting leader Iovation, and led go-to-market programs for machine identity management pioneer Venafi.

Robert Wagner - NCFTA
Title: Overcoming The CyberSecurity Poverty Line; Democratizing Security for Everyone

Bio: Robert Wagner is the Field CISO at Fletch.ai. He's a highly respected security advisor and strategist. With almost 20 years of blue team experience, he has helped organizations of all sizes around the globe improve their security programs and reduce their risk profiles. His security experience ranges from a hands-on keyboard SOC analyst at ABN Amro, through Security Architect at TransUnion, and Global Security Strategist at Splunk. He has presented and taught at Information Security and Hacker conferences ranging from DefCon, APIsecure, Bsides Tel Aviv, GrrCon, Dawn or Doom, WCISC, and more. He is a co-founder of the not-for-profit organization Hak4Kidz, serves on the board of the Chicago ISSA chapter, and regularly volunteers for various Bsides and other hacker cons.

Abstract: Today, the cyber risks organizations face are more complex and imminent than ever before. Organizations must balance the need to drive digital innovation with the cost of potential cyber threats and data breaches, while also streamlining costs and processes. This is a difficult feat, especially when there are so many challenges that prevent smaller companies from accessing affordable security software.

This talk will provide insight on why smaller companies struggle with security costs and offer strategies to overcome these challenges.

Yongge Wang - UNCC CCI
Bio: Dr. Yongge Wang is a professor at UNC Charlotte. Dr. Wang has published extensively on research topics including algorithmic information theory, cryptography, and post-quantum security. Dr. Wang has proved several classical results in modern effective randomness research which are included as the fundamental theorems in most Algorithmic Information Theory graduate textbooks. Dr. Wang is the holder of three patents and the inventor of two IEEE 1363 standardized techniques. Dr. Wang is one of the designers for fundamental W3C and IETF XML securitytechniques such as XMLENC and XMLDSig syntax. These standards are the starting point for all XML related security techniques. Dr. Wang played important roles in developing research and education programs at UNC Charlotte. Recently, Dr. Wang has been working on fully homomorphic encryption, garbled computation techniques, and apply these techniques to achieve privacy preserving computation in cloud. Dr. Wang has designed quantum resistant public key encryption techniques RLCE (http://quantumca.org) and developed the software package readily to be integrated into current Internet infrastructure. Dr. Wang has developed the 4-step UNCC patented BDLS Byzantine Fault Tolerance protocol for blockchains. Dr. Wang is currently an academic advisor for the Cryptic Labs http://crypticlabs.org that builds a unique community of illustrious cryptography and security advisors, researchers and innovative blockchain entrepreneurs who work on decentralize and distributed trust.

Kurt Wassersug - Sepio

Bio: Kurt Wassersug of Sepio brings over 20 years of leadership experience and has worked in a myriad of cyber and InfoSec companies during his tenure. He has worked with some of largest global companies and has a deep understanding of operational and technical challenges security practitioners face. Kurt is a senior manager at Sepio, a company focused on providing complete visibility using Layer 1 of the OSI model. Layer 1 focuses on the existence of a device and can stop attacks instantly where traditional visibility tools use layer 2 (MAC) and layer 3+ (TCP/IP) network data to discover and identify devices. This is problematic as at Layers 2 and above, devices without a digital existence (passive taps, unmanaged switches, MiTM attacks or "spoofed" devices) go undetected.

Howard Whyte - Truist Financial Corporation
Bio: Howard Whyte is an Executive Vice President and the Chief Information Security Officer (CISO) at Truist Financial Corporation. As CISO, Mr. Whyte is responsible for execution of the Corporation's Information Security Program and alignment with enterprise programs and business objectives, ensuring that information assets and technologies are protected.

Prior to joining Truist in January 2022, Mr. Whyte served as CISO at Boeing, where he was responsible for the protection of Boeing's information and computing resources globally and for managing information technology risk. Earlier, Mr. Whyte worked for more than 20 years as an executive leader of information technology and security in the federal government, military, and private sector. He served as the Chief Information Officer and Chief Privacy Officer at the Federal Deposit Insurance Corporation (FDIC), where he acted as an advisor to the chairman, board members, and senior executives on all strategic issues relating to information technology, including governance, investments, program management, strategic planning, and security. Previously, he was the CISO at FDIC and worked to reduce cybersecurity risk by implementing an around-the-clock security operations center and incorporating threat intelligence into security operations. In addition, he led the Threat Management Center at Goldman Sachs, focusing on cybersecurity detection, protection, response, and recovery on a global scale. He also served as the CISO and deputy CISO at NASA, where he provided direction and future vision on a wide range of information technology solutions for mission and corporate system .

Earlier in his career, he was a senior information officer in the U.S. Army Network Enterprise Technology Command and the Defense Information Systems Agency; a telecommunications manager at Interim HealthCare; and an information management officer in the U.S. Army.

Mr. Whyte's primary area of responsibility for Truist includes managing and overseeing the Corporate Cyber Security Department, which consists of Cyber Operations; Vulnerability Management and Data Protection; Identity and Access Management; Cyber Governance, Risk, and Compliance; Cyber Architecture and Strategy; Cyber Strategic Initiatives and Shared Services Management; as well as the Divisional CISOs, who serve as security liaisons to the business. Mr. Whyte holds a Bachelor of Science degree in Management Studies from the University of Maryland and a Master of Business Administration from the University of Phoenix.

SA Katherine Wise - FBI
Bio: SA Katherine Wise joined the FBI in January 2018 and was assigned to the Charlotte Field Office where she has investigated violent crimes against children, human trafficking and computer intrusions. SA Wise is a member of the Charlotte Cyber Task Force, which is responsible for both criminal and national security computer intrusion investigations. Prior to joining the FBI, she worked in the Private Sector a Cyber Incident Responder on the Global Cyber Security team where she was responsible for responding to incidents ranging from Business Email Compromises to Nation State actors.

Sounil Yu - JupiterOne
Title: New Paradigms for the Next Era of Security

Bio: Sounil Yu is the CISO and Head of Research at JupiterOne. He created the Cyber Defense Matrix and the DIE Triad, which are reshaping approaches to cybersecurity. He's a Board Member of the FAIR Institute; co-chairs Art into Science: A Conference on Defense; is a visiting fellow at GMU Scalia Law School's National Security Institute; teaches at Yeshiva University; and advises many startups. Sounil previously served as the CISO-in-Residence at YL Ventures and Chief Security Scientist at Bank of America. Before Bank of America, he helped improve information security at several Fortune 100 companies and Federal Government agencies. Sounil has over 20 granted patents and was recognized as one of the most influential people in security in 2020 by Security Magazine, Influencer of the Year in 2021 by SC Awards, and a 2021 Top 10 CISO by Black Unicorn Awards. He has an MS in Electrical Engineering from Virginia Tech and a BS in Electrical Engineering and a BA in Economics from Duke University.

Abstract: The onslaught of ransomware has undermined our ability to maintain the confidentiality, integrity, and availability (CIA) of our data. As attackers refine and mature their techniques to drive irreversible outcomes, we must look at how we can become more resilient. But is securing everything by design the best way to go about it? This session advocates that we need to move away from the CIA Triad to a new paradigm, called the DIE Triad, which enables us to truly be resilient against irreversible attacks.

UNIVERSITY OF NORTH CAROLINA
CHARLOTTE
COLLEGE OF COMPUTING
AND INFORMATICS

In collaboration with

ISSACharlotte
Information Systems Security Association

2022 Cybersecurity Symposium

THANK YOU TO OUR SPONSORS

Title

Bank of America

Silver

LOWE'S

NETSPI™

WELLS FARGO

TIAA

noname

SentinelOne

SEPIO

BeyondTrust

ally

Bronze

netskope

eclypsium

DUKE ENERGY

Exhibitor / SMB

tenable

Abnormal

Booz | Allen | Hamilton
100 YEARS

huntsource
Pinpointing technology talent.

GreerWalker
CPAs & Advisors

INTERNETWORK ENGINEERING