FAIR22

CONFERENCE

SCALE | RISK MANAGEMENT TO THE NEXT LEVEL

FAIR INSTITUTE

TABLE OF
CONTENTS

THE CHAIRMAN'S
WELCOME

As FAIR has won widespread acceptance as an industry standard, we're looking ahead to what's next. The theme of the 2022 FAIR Conference is Scale – elevating our expectations and practices to maximize the positive impact across our organizations of the FAIR model and mindset.

You'll hear from industry leaders with insights into culture changes that open the way to a successful quantitative risk management program, as well as tips on the step-by-step foundational work.

A highlight of this year's conference will be sessions on the FAIR Controls Analytics Model (FAIR-CAM™), a look into the future of risk management when automated, risk-based controls systems will run on sound risk measurement.

As always, FAIRCON22 will be a place of community, where you'll have an opportunity to meet in person, establish trusted conversations and aid one another in taking our profession to a higher level.

JACK JONES
CHAIRMAN, FAIR INSTITUTE

IMPORTANT INFORMATION

QUESTIONS:

Ask questions in-person or visit **faircon22.com/questions** to submit.

AGENDA:

Schedules are subject to change.
Visit **fairinstitute.org/faircon22-agenda** for the most up-to-date agenda information.

DAY ONE

All Times in EDT (UTC−04:00)	Session Information		
7:30 - 9:00 AM	*Registration and Breakfast*		
9:00 - 10:00 AM	**Welcome Remarks and Opening Keynote** **How Risk Economics Can Help Us Win the Battle in Cyberspace** Larry Clinton, President, ISA		
10:00 - 10:45 AM	**Panel: Driving Culture Change - From a Compliance to a Risk-based Approach to Cybersecurity** *Moderator: Omar Khawaja, CISO, Highmark Health* Mark Tomallo, SVP, CISO, Victoria's Secret Mary Elizabeth Faulkner, CISO, Thrivent Financial Jeff Norem, Deputy CISO, Freddie Mac		
10:45 - 11:15 AM	*30-Minute Networking and Exhibitor Break*		
11:15 AM - 12:00 PM	**Presentation: Subjective Judgements: Outperforming Your Current Best Experts** Douglas Hubbard, President, Hubbard Decision Research		
12:00 - 1:00 PM	*Lunch and Exhibitor Break*		
	Track 1	**Track 2**	**Track3**
1:00 - 1:45 PM	**Case Study: "FAIR: Okay, Now What?" - Steps to Set Up a Quantitative Risk Management Program at Any Organization** Michael Meis, Associate CISO, KU Health	**Presentation: How to Scale FAIR Programs with Controls Analytics** Bryan Smith, CTO, RiskLens Jack Jones, Chairman FAIR Institute, Chief Risk Scientist RiskLens	**Presentation: How Partnering with CISA Can Help Your Organization Better Manage Your Risk** Mona Harrington, Acting Assistant Director, National Risk Management Center, CISA, & Fmr. CISO, U.S. Elections Assistance Commission
1:45 - 2:15 PM	*30-Minute Networking and Exhibitor Break*		

DAY**ONE**

TUESDAY
SEPTEMBER 27

	Track 1	Track 2	Track3
2:15 - 3:00 PM	**Case Study: Five Objections to FAIR and How to Overcome Them** Tony Martin-Vegue, Senior Information Security Risk Engineer, Netflix Prashanthi Koutha, Senior Risk Engineer, Netflix	**Case Study: Harnessing The Voltage Effect to Scale our FAIR Risk Programs** Zach Cossairt, Information Risk Program Manager, Equinix	**Fireside Chat: A Legislative and Policy Update on Cybersecurity and Risk Management** Moderator: Larry Clinton, President, ISA Mark Montgomery, Executive Director, CyberSolarium.org Frank Cilluffo, Distinguished Advisor, CSC 2.0
3:00 - 3:30 PM	*30-Minute Networking and Exhibitor Break*		
3:30 - 4:15 PM	**Case Study: Embedding CRQ in the Infosec Governance Process of a Fast-Growing Pop Culture Retail Organization** Markus Kaufmann, CISO, Senior Director of Information Security, Funko Tom Callaghan, Co-Founder, C-Risk	**Case Study: Scaling M&A Cyber Due Diligence Efforts with FAIR** Cedric de Carvalho, Head of Group Cyber Risk & Advisory, Richemont	**Presentation: Trends in Determining Systemic Cyber Risk for the Financial Services Industry** Matthew Tolbert, Senior Cybersecurity Specialist, United States Federal Reserve
4:15 - 5:00 PM	**Presentation: Getting Your Money's Worth: Putting Your Controls Inventory to Work** Marta Palanques, Director of Risk Methodologies, Technology Risk Management, Capital One	**Presentation: Unveiling the IRIS 2022: Bigger Scale, Greater Depth, and More Data for Your CRQ Program** Wade Baker, Partner, Cyentia Institute David Severski, Senior Security Data Scientist, Cyentia Institute	**Presentation: Justifying the Value of Cybersecurity to the Business with Highmark Health and the BOSITE Framework** Omar Khawaja, CISO, Highmark Health
6:00 - 9:00 PM	**Social Event** The Grill, at the Wharf 99 Market Square SW, Washington, D.C., DC 20024		

4

DAYTWO

WEDNESDAY
WEDNESDAY
SEPTEMBER 28

All Times in EDT (UTC–04:00)	Session Information		
7:30 - 9:00 AM	*Registration and Breakfast*		
9:00 - 9:45 AM	**Welcome and Keynote Address Trusting Risk-Informed Decisions** Jack Jones, Chairman, FAIR Institute		
9:45 - 10:45 AM	**Panel: Communicating Cyber Risk to the Board and the Business: How Is It Changing?** *Moderator: Julian Meyrick, Managing Partner & Vice President, Security Strategy Risk & Compliance, Security Services, IBM* James Lam, Board Director & ERM Author Michael Meis, Associate CISO, KU Health Evan Wheeler, Sr. Director, Technology Risk Management, Capital One		
10:45 - 11:15 AM	*30-Minute Networking and Exhibitor Break*		
11:15 AM - 12:00 PM	**Presentation: Managing Cyber Risk as a Strategic Enterprise Risk** John Button, Principal Enterprise Risk Advisor, Gartner		
12:00 - 1:45 PM	**2022 FAIR Awards Ceremony and Luncheon**		
	Track 1	**Track 2**	**Track3**
1:45 - 2:30 PM	**Presentation: Expedia Groups' Approach to Build an Effective Security Risk Management Program using FAIR** Krishna Sheshabhattar, Director, Security, Risk, and Compliance, Expedia Group Randy Spusta, Global Competency Leader, Security Strategy Risk & Compliance Practice, IBM Security	**Case Study: Quantifying the Control and Risk Landscape Using FAIR-CAM** Tyler Britton, Quantitative Cyber Risk Manager, DropBox	**Fireside Chat: What the Revised SEC Guidance on Cyber Risk Disclosures Means for You** David Hirsch, Chief of the Crypto Asset and Cyber Unit, Division of Enforcement, SEC Kristy Littman, Fmr. Chief of Enforcement - Cyber Unit, SEC

DAYTWO

	Track 1	Track 2	Track3
2:30 - 3:15 PM	**Presentation: Scaling FAIR for Third Party Risk Management** Bob Maley, Chief Security Officer, Black Kite	**Case Study: Refining the "R" in GRC at Scale** Michael Radigan, Cyber Risk Advisor, Cisco	**Presentation: Risk Quantification for Practitioners** Kyle Burk, CISO, Archer
3:15 - 3:45 PM	*30-Minute Networking and Exhibitor Break*		
3:45 - 4:30 PM	**Case Study: Building a Strong Foundation for your Quantitative Risk Management Program** Tim Wynkoop, Sr. Information Security Risk Engineer, Equinix	**Panel: Scaling a Quantitative Risk Management Program** Andrew Retrum, Managing Director, US Security Program & Strategy Practice Lead, Protiviti David Severski, Senior Security Data Scientist, Cyentia Institute Matt Kruse, VP Corporate Programs, FIS Global Tim Kelly, Senior Manager, Protiviti	**Panel: CIS, NIST 800-53, ISO27000 - Mapping Leading Control Frameworks to FAIR-CAM™** Moderator: Jack Jones, Chairman, FAIR Institute Daniel Stone, Associate Director, Security & Privacy, Protiviti Erin Macuga, Manager Risk and Information Security, Thrivent Financial Robert Immella, Global Leader of Cyber Risk Quantification, Caterpillar Inc Tyler Britton, Quantitative Cyber Risk Manager, DropBox Drew Brown, Information System Security Developer, FAA
4:30 - 5:00 PM	**Closing Remarks**		

THANKS TO OUR
SPONSORS

TECHNICAL ADVISOR

RiskLens®

FAIR INSTITUTE SPONSORS

riskrecon
mastercard.

Founding Advisory Partner

protiviti®
Face the Future with Confidence

IBM

ARCHER

FAIRCON22 SPONSORS

BLACK KITE

THE Open GROUP

metricstream

LOGICGATE

119
Cyentia
INSTITUTE

EVENT
SPEAKERS

SPEAKERS

WADE BAKER
CO-FOUNDER, CYENTIA INSTITUTE

Dr. Wade Baker is a Co-Founder of the Cyentia Institute, which focuses on improving cybersecurity knowledge and practice through data-driven research. He's also a professor in Virginia Tech's College of Business, working to prepare the next generation of industry leaders. Prior to this, Wade held positions as the VP of Strategy at ThreatConnect and was the CTO of Security Solutions at Verizon, where he had the great privilege of leading Verizon's Data Breach Investigations Report (DBIR) research team for 8 years.

TUESDAY
4:15 - 5:00 PM

Unveiling the IRIS 2022: Bigger Scale, Greater Depth, and More Data for your CRQ Program

TYLER BRITTON
QUANTITATIVE CYBER RISK MANAGER, DROPBOX

Tyler Britton is the Staff Cyber Risk Manager at Dropbox, and is currently building a FAIR based risk program in Dropbox's security organization. Previous to Dropbox, he has worked as a risk consultant, information security analyst, software engineer, and teacher. He's passionate about digital privacy, improving the cyber risk industry, and finding good solutions to difficult security problems. When he's not working, you might find Tyler losing a game of chess, suffering through a yoga pose, trying to stay awake while reading, cursing mosquitos on his way up a mountain, or missing his archery target. He lives in a small resort town in northern Idaho with his wife and two young boys.

WEDNESDAY
1:45 - 2:30 PM

Quantifying the Control and Risk Landscape Using FAIR-CAM

3:45 - 4:30 PM

CIS, NIST 800-53, ISO27000 - Mapping Leading Control Frameworks to FAIR-CAM™

SPEAKERS

DREW BROWN
INFORMATION SYSTEM SECURITY DEVELOPER, FAA

Drew is a resourceful technology consultant with over 20 years of experience developing solutions with state and federal government, as well as small businesses and Fortune 500 companies. His expertise includes: Cybersecurity governance, putting the "Sec" in DevOps (development), Project management, Design and implementation of numerous infrastructure platforms, focusing on total cost of ownership and minimizing the impact of change. Drew specializes in developing cyber threat analysis programs and implementing risk management programs, including quantitative risk analysis that reduced audit findings.
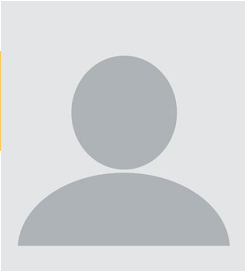
WEDNESDAY
3:45 - 4:30 PM

Mapping Leading Control Frameworks to FAIR-CAMTM

KYLE BURK
CISO, ARCHER

Ti dit posae. Ficim sinvell aborece ssimus.

Bo. Itati res seque volorere vellita tinulli quostiusa quam, testium et quias dolupta amus, si ommolessus eiure, sum etur?

Nam, cuptaepro consequid qui dolorit asperum atur?

Inis minima core lacepe sum quaerum nus, tem utem natur sundis et quatio. Et inctur re cores es ut molorerum ratiusdae prorion sequatia se voluptae nis et, verum alibus modit lit mo eiumque eum velest quat escimagnihic to bera quassim odipsamus volorem aut maio eseribus ipis apernatur?

WEDNESDAY
1:45 - 2:30 PM

What the Revised SEC Guidance on Cyber Risk Disclosures Means for You

SPEAKERS

JOHN BUTTON
PRINCIPAL ENTERPRISE RISK ADVISOR, GARTNER

John Button is a Gartner Enterprise Risk Advisor, advising enterprise risk management leaders and practitioners on all aspects of ERM. He has 14 years of experience as a risk advisor, consultant, and practitioner. Prior to joining Gartner six years ago, John was a risk management consultant at Deloitte, NTT DATA, SRA (now General Dynamics.) His engagements included DHS, OPM, CFPB, FEMA, Options Clearing Corporation, and Texas DOT. His work focused on enterprise risk, cyber security, and NIST RMF and SP 800-53 control selection and implementation. John is a published author multiple times over and the managing editor of several books including Cultural Calamity, The Tao of Risk Management, and The Drone Age.

WEDNESDAY
11:15 AM - 12:00 PM

Managing Cyber Risk as a Strategic Enterprise Risk

TOM CALLAGHAN
CO-FOUNDER, C-RISK

Mr Tom Callaghan is the Co-Founder of C-Risk, the European authority in the quantification of cyber risk in financial terms. He is also co-chair of the Paris FAIR Institute chapters. Tom has almost 30 years' experience managing Enterprise information technology and prior to founding C-Risk he was an executive at Dell holding various leadership positions. Tom studied Economics and Computer Science at University College Cork, Ireland and holds multiple industry certifications including Open FAIR.

TUESDAY
3:30 - 4:15 PM

Embedding CRQ in the Infosec Governance Process of a Fast-Growing Pop Culture Retail Organization

SPEAKERS

FRANK CILLUFFO
DISTINGUISHED ADVISOR, CSC 2.0

Cilluffo is a member of the Cyberspace Solarium Commission and the Department of Homeland Security's Advisory Council, and he's routinely called upon to advise senior officials in the executive branch, U.S. Armed Services, and state and local governments on an array of matters related to national and homeland security strategy and policy. In addition to briefing Congressional committees and their staffs, he has publicly testified before Congress on numerous occasions, serving as a subject matter expert on policies related to cyber threats, counterterrorism, security and deterrence, weapons proliferation, organized crime, intelligence and threat assessments, emergency management, and border and transportation security. Similarly, he works with U.S. allies and organizations such as NATO and Europol. He has presented at a number of bi-lateral and multi-lateral summits on cybersecurity and countering terrorism, including the U.N. Security Council.

TUESDAY
2:15 - 3:00 PM

A Legislative and Policy Update on Cybersecurity and Risk Management

LARRY CLINTON
PRESIDENT & CEO, INTERNET SECURITY ALLIANCE

Larry Clinton leads a diverse board of directors consisting of 20 senior cyber practitioners (typically CISO/CIO) representing nearly every critical industry sector toward ISA's mission. ISA's Mission is to integrate advanced technology with economics and public policy to help build a sustainable system of cybersecurity. ISA pursues 3 major goals: 1) to promote thought leadership on cybersecurity; 2) to advocate for public policy that will help build a sustainably secure cyber system; and 3) to promote the use of effective standards and practices for cybersecurity. Sectors represented on the ISA board include agriculture, audit, banking, communications, defense, education, financial services, healthcare, insurance, manufacturing, media, retail, software development, technology, and utilities.

TUESDAY
9:00 - 10:00 AM

How Risk Economics can Help Us Win the Battle in Cyberspace

2:15 - 3:00 PM

A Legislative and Policy Update on Cybersecurity and Risk Management

SPEAKERS

ZACH COSSAIRT
INFORMATION RISK PROGRAM MANAGER, EQUINIX

Zach is the Information Risk Program Manager at Equinix, the world's leading digital infrastructure company. He received his undergraduate degree in security and risk analysis from Pennsylvania State University and now studies the intersection of psychology and decision-making in the behavioral economics master's program at the Chicago School of Professional Psychology. He served nearly a decade in the United States Navy and spent his sea tour onboard the fast attack submarine USS Pasadena as a Fire Control Technician, responsible for collecting, aggregating, and synthesizing various forms of intelligence data to inform the tactical and strategic decision-making of command and squadron leadership. Upon exiting the Navy after his shore tour as an instructor and training specialist, Zach held multiple positions assessing risk in both the public and private sectors before transitioning into his current role at Equinix.

TUESDAY
2:15 - 3:00 PM

Harnessing The Voltage Effect to Scale our FAIR Risk Programs

CEDRIC DE CARVALHO
HEAD OF GROUP CYBER RISK & ADVISORY, RICHEMONT

Cedric De Carvalho is a cybersecurity enthusiast and a risk professional who strives to help the executives to find the right balance between agile business growth and protecting the business. With 10 years of experience within various cybersecurity position, he developed a pragmatic approach to cyber risk management, which he believes should be less judgmental and more based on a scientific approach.

TUESDAY
3:30 - 4:15 PM

Scaling M&A Cyber Due Diligence Efforts with FAIR

SPEAKERS

MARY ELIZABETH FAULKNER
SVP & CISO, THRIVENT FINANCIAL

TUESDAY
10:00 - 10:45 AM

Driving Culture Change - From a Compliance to a Risk-based Approach to Cybersecurity

Mary Elizabeth Faulkner is VP and Chief Information Security Officer (CISO) for Thrivent and serves in this role for Thrivent, its subsidiaries and affiliates.

As the CISO, Mary Elizabeth is responsible for leading teams to execute the Information Security strategy, provide management and oversight, support Cyber Defense Engineering, Identity and Access Management Engineering, Incident Response, and Information Assurance Services.

Prior to joining Thrivent, Mary Elizabeth was CISO at a manufacturing and retail global organization. In addition, she has led global IT organizations driving maturity in information security, network, and security operations. She has over 25 years of experience in Information Security, Litigation Advisory Services, and Audit. Mary Elizabeth has served a number of industries in security advisory roles to include technology, insurance, retail, gaming, government, automotive, and manufacturing.

MONA HARRINGTON
ACTING ASSISTANT DIRECTOR,
NATIONAL RISK MANAGEMENT CENTER, CISA

TUESDAY
1:00 - 1:45 PM

How Partnering with CISA Can Help Your Organization Better Manage Your Risk

Mona Harrington serves as the (Acting) Assistant Director for National Risk Management Center (NRMC) at the Cybersecurity and Infastructure Security Agency (CISA). As the the (Acting) Assistant Director for NRMC, she identifies opportunities for collaboration with public-private partners to mitigate cyber and physical risk to National Critical Functions where those functions of the government and private sector are so vital to the United States that any disruption, corruption, or dysfunction would have a debilitating affect on security, national economic security, national public health or safety, or any combination thereof. She also oversees efforts to facilitate a strategic, cross-sector risk management approach to cyber and physical threats to critical infrastructure.

SPEAKERS

DAVID HIRSCH

CHIEF OF THE CRYPTO ASSET AND CYBER UNIT, DIVISION OF ENFORCEMENT, SEC

Dave Hirsch J.D., CFE, is Chief of the Crypto Asset and Cyber Unit within the SEC Division of Enforcement. Prior to that he served as Counsel to SEC Commissioner Caroline Crenshaw, where he was primarily responsible for matters relating to enforcement along with digital assets and cybersecurity. He began his career with the SEC as Counsel in the Division of Enforcement, and was a member of the SEC Digital Ledger Technology Working Group and the Dark Web Working Group. Dave is a graduate of the UCLA School of Law and clerked for Judge Edward J. Schwartz in the United States District Court for the Southern District of California. Before joining the SEC, he was a litigator, and later co-founded and ran a private investigation firm focused on securities fraud investigations. He authored the chapter on Blockchain and Information Security in the Handbook of Blockchain Law.

WEDNESDAY
1:45 - 2:30 PM

What the Revised SEC Guidance on Cyber Risk Disclosures Means for You

DOUG HUBBARD

PRESIDENT, HUBBARD DECISION RESEARCH

Mr. Hubbard is the inventor of the powerful Applied Information Economics (AIE) method. His management consulting career started 32 years ago with Coopers & Lybrand, focusing on the application of quantitative methods. The last 22 years he has completed over 160 projects for the application of AIE to solve current business issues in many areas including IT benefits and risks including cybersecurity, engineering risks, market forecasts for pharma and medical devices, environmental policy, mergers & acquisitions, Silicon Valley startups, the likelihood of success of new movies, and military logistics to name a few. His AIE methodology has received critical praise from Gartner, Forrester, and others.

TUESDAY
11:15 AM - 12:00 PM

Subjective Judgements: Outperforming Your Current Best Experts

SPEAKERS

ROBERT IMMELLA
GLOBAL LEADER OF CYBER RISK QUANTIFICATION, CATERPILLAR INC.

Robert has 20 years in Information Technology as Director of IT and Project Manager. For the past 5 years, he has focused on Cyber Risk Quantification, specializing in the FAIR methodology, cybersecurity controls, and building CRQ programs. Robert is on the RiskLens Technical Advisory Board and he is a previous FAIRCON presenter.

WEDNESDAY
3:45 - 4:30 PM

CIS, NIST 800-53, ISO27000 - Mapping Leading Control Frameworks to FAIR-CAM™
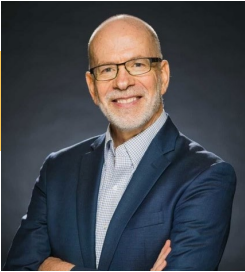
JACK JONES
CHAIRMAN, FAIR INSTITUTE

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.

TUESDAY
1:00 - 1:45 PM

How to Scale FAIR Programs with Controls Analytics

WEDNESDAY
9:00 - 9:45 AM

Trusting Risk-Informed Decisions

3:45 - 4:30 PM

CIS, NIST 800-53, ISO27000 - Mapping Leading Control Frameworks to FAIR-CAM™

SPEAKERS

MARKUS KAUFMANN
CISO, SR. DIRECTOR OF INFORMATION SECURITY, FUNKO

Markus Kaufmann is the current Sr. Director of Information Security and Compliance at Funko LLC. Markus came to Funko as Information Security Professional with over 30 years of experience in IT. Leveraging his broad exposure to technology via various engineering, support, and architecture roles, Markus has made Information Security his primary focus for the past 15 years. In his current role at Funko, he is working to build and mature the company's Information Security and Compliance programs, using the Factor Analysis of Information Risk (FAIRTM)assessment methodology as a foundational tool to ensure the programs remain focused on areas critical to the company's success.

TUESDAY
3:30 - 4:15 PM

Embedding CRQ in the Infosec Governance Process of a Fast-Growing Pop Culture Retail Organization

TIM KELLY
SENIOR MANAGER, PROTIVITI

Tim is a Senior Manager in the Protiviti Chicago office, specializing in cyber risk quantification and risk management program development. He has experience performing quantitative risk assessments, developing, and implementing risk management programs, and performing cybersecurity program and strategy assessments.

WEDNESDAY
3:45 - 4:30 PM

Scaling a Quantitative Risk Management Program

SPEAKERS

OMAR KHAWAJA
CISO, HIGHMARK HEALTH

Omar Khawaja serves as the Vice President, Chief Information Security Officer for Highmark Health, an $18 billion national, blended health organization that includes one of America's largest Blue Cross Blue Shield insurers and a growing regional hospital and physician network. Based in Pittsburgh, Pa., Highmark Health's 35,000 employees serve millions of customers nationwide through the nonprofit organization's affiliated businesses including Highmark Inc., Allegheny Health Network, HM Insurance Group, United Concordia Dental, HM Health Solutions and HM Home & Community Services. Omar currently serves on the boards of: HITRUST, Leadership Pittsburgh, Action Housing and FAIR Institute; on the Governing Body of Evanta; on the CISO Workgroup of BCBSA; and adjunct faculty for the CISO program at Carnegie Mellon University. In addition, he serves as an advisor to half a dozen tech firms

TUESDAY
10:00 - 10:45 AM

Driving Culture Change - From a Compliance to a Risk-based Approach to Cybersecurity

4:15 - 5:00 PM

Justifying the Value of Cybersecurity to the Business with Highmark Health and the BOSITE Framework

PRASHANTHI KOUTHA
SENIOR RISK ENGINEER, NETFLIX

Prashanthi Koutha is a cybersecurity risk analyst with over five years of experience enabling risk-based decisions across the business. Koutha holds an MS in Information Technology Management from the University of Texas at Dallas and holds the OpenFAIR Analyst industry certification. She is also a member of the RiskLens Technical Advisory Board: a platform that offers quantitative cyber risk management solutions built on the FAIR standard.

TUESDAY
2:15 - 3:00 PM

Five Objections to FAIR and How to Overcome Them

SPEAKERS

MATT KRUSE
VP CORPORATE PROGRAMS, FIS GLOBAL

Matt Kruse is the Enterprise Risk Management senior director. In this role, Matt leads an experienced, global team of project managers, reporting analysts and systems developers to implement the strategic and operational objectives of the Risk, Information Security and Compliance organization. He is responsible for establishing the risk management framework and policy that keeps FIS' risk-taking activities in line with its strategic objectives and risk appetite.

WEDNESDAY
3:45 - 4:30 PM

Scaling a Quantitative Risk Management Program

JAMES LAM
BOARD DIRECTOR & ERM AUTHOR, JAMES LAM ASSOCIATES

James C. Lam is a risk management consultant and board director. He is president of James Lam & Associates, a risk management consulting firm he founded in 2002. His clients include corporate directors and executives across key sectors, including financial services, energy, technology, healthcare, government entities, and non-profits. He currently serves as independent board director and audit committee chair of RiskLens and a board director of the FAIR Institute. Previously, James served as chair of the board, audit committee, and compliance committee at Recology and chair of the risk committee and member of the audit committee at E*TRADE Financial (NASDAQ: EFTC).

WEDNESDAY
9:45 - 10:45 AM

Communicating Cyber Risk to the Board and the Business: How Is It Changing?

SPEAKERS

KRISTINA LITTMAN
PARTNER, LITIGATION DEPARTMENT, WILLKIE FARR & GALLAGHER, LLP
FMR. CHIEF OF ENFORCEMENT – CYBER UNIT, SEC

Kristina Littman is a partner in the Litigation Department and a member of the Securities Litigation & Enforcement Practice Group. Kristy represents corporations, registrants, and individuals in complex disputes, including regulatory enforcement and white-collar defense. She also counsels clients on cryptocurrency and digital assets regulation and cybersecurity matters, including investigations and enforcement actions by financial regulators. Kristy previously served as the Chief the Crypto Assets and Cyber Unit in the Division of Enforcement of the U.S. Securities and Exchange Commission (SEC). In that role, she led a group of attorneys and specialists across the nation responsible for investigating and litigating violations of the federal securities laws relating to digital assets, cybersecurity, and cyber-related trading violations.

WEDNESDAY
1:45 - 2:30 PM

What the Revised SEC Guidance on Cyber Risk Disclosures Means for You

ERIN MACUGA
MANAGER RISK AND INFORMATION SECURITY, THRIVENT FINANCIAL

Erin is the Manager of Information Security Risk Management for Thrivent. As the Manager, Erin is responsible for leading the team to conduct and analyze risks related to assets, threats, and impacts using an industry leading quantifiable methodology. Erin is responsible for leading team members in collecting threat intelligence across various platforms and feeds, providing analysis, and communicating across all internal stakeholders for an actionable response. She drives efforts to equip business leaders with information to make risk-informed decisions and to address vulnerabilities in a timely manner.

WEDNESDAY
3:45 - 4:30 PM

CIS, NIST 800-53, ISO27000 - Mapping Leading Control Frameworks to FAIR-CAM™

SPEAKERS

BOB MALEY
CHIEF SECURITY OFFICER, BLACK KITE

Bob has been involved in security for most of his career, initially in physical security as a law enforcement officer. In those years Bob acquired a broad range of expertise and experience in all areas of security, including third-party security, risk assessment, architecture, design, policy development, deployment, incident response and investigation and enterprise solution deployments in areas including intrusion detection, data protection, compliance, and incident reporting and response.

WEDNESDAY
2:30 - 3:15 PM

Scaling FAIR for Third Party Risk Management

TONY MARTIN-VEGUE
SENIOR INFORMATION SECURITY RISK ENGINEER, NETFLIX

Tony Martin-Vegue is a writer, speaker, and risk expert with a passion for data-driven decision-making. He uses his expertise in economics, cyber risk quantification, and information security to advise senior operational and security leaders on integrating evidence-based risk analysis into business strategy. Martin-Vegue formerly served on the Society of Information Risk Analysts board and is the co-chair of the San Francisco chapter of the FAIR Institute—2 professional organizations dedicated to advancing risk quantification.

TUESDAY
2:15 - 3:00 PM

Five Objections to FAIR and How to Overcome Them

SPEAKERS

MICHAEL MEIS
ASSOCIATE CISO, KU HEALTH

Michael is an Army veteran with over 13 years' experience and a passion for architecting security programs, leading people, and developing world-class security teams. During his career, Michael partnered with the USDA CISO to develop one of the largest consolidations of security services in the federal government. Michael also led the H&R Block Information Security team through a transformation of their GRC operations to instill quantitative cyber risk management practices. Michael currently leads The University of Kansas Health System Cybersecurity team as they protect the critical systems, data, and people that provide lifesaving patient care.

TUESDAY
1:00 - 1:45 PM

"FAIR: Okay, Now What?" - Steps to Set Up a Quantitative Risk Management Program at Any Organization

WEDNESDAY
9:45 - 10:45 AM

Communicating Cyber Risk to the Board and the Business: How Is It Changing?

JULIAN MEYRICK
MANAGING PARTNER & VICE PRESIDENT, SECURITY STRATEGY RISK & COMPLIANCE, SECURITY SERVICES, IBM

Julian Meyrick is the Managing Partner & Vice President for IBM Security's worldwide Security Strategy Risk & Compliance practice. IBM Security is the fastest-growing enterprise IT security company in the world.

In his leadership role, Julian helps clients develop their security strategy in the context of the cyber business risk that they face; he has a particular focus on advising boards on the potential business impact of cybersecurity, and on quantifying cybersecurity risk in financial terms. Julian is passionate about attracting talent into the cybersecurity profession and is a member of the UK National Cyber Security Centre's Industry Advisory Board for their CyberFirst programme. Julian is IBM's executive sponsor for the Charter of Trust, a unique initiative by leading global companies to secure the digital world. Julian is also a member of the FAIR Institutes Industry Advisory Board.

WEDNESDAY
9:45 - 10:45 AM

Communicating Cyber Risk to the Board and the Business: How Is It Changing?

SPEAKERS

MARK MONTGOMERY
EXECUTIVE DIRECTOR, CYBERSOLARIUM.ORG

Mark Montgomery is the Senior Director of the Center on Cyber and Technology Innovation and a Senior Fellow at the Foundation for Defense of Democracies. He serves as the Executive Director of Cybersolarium. org, a non-profit organization which works to implement the recommendations of the Cyberspace Solarium Commission, where he was Executive Director from 2019 to 2021. Prior to this, Mark was Policy Director for the Senate Armed Services Committee under the leadership of Senator John S. McCain and completed 32 years as a nuclear trained surface warfare officer in the U.S. Navy, retiring as a Rear Admiral in 2017.

TUESDAY
2:15 - 3:00 PM

A Legislative and Policy Update on Cybersecurity and Risk Management

JEFF NOREM
DEPUTY CISO, FREDDIE MAC

Jeff is a data protection and privacy leader, CISO, board member and cyber product adviser with 20+ years of experience in security, privacy, fraud and risk management across multiple industries. He is a speaker at global security and risk conferences, author and active member in the community.

Jeff holds an MBA from the University of St. Thomas with a focus in the risk leadership, is a founding member of the UST Risk Leadership Advisory Board.

His focus is building security programs that allow organizations to meet their objectives through effective decision making and prioritized security investments by understanding their risk in terms of probability of financial loss.

TUESDAY
10:00 - 10:45 AM

Driving Culture Change - From a Compliance to a Risk-based Approach to Cybersecurity

SPEAKERS

MARTA PALANQUES
DIRECTOR OF RISK METHODOLOGIES, TECHNOLOGY RISK MANAGEMENT, CAPITAL ONE

TUESDAY
4:15 - 5:00 PM

Getting Your Money's Worth: Putting Your Controls Inventory to Work

Marta Palanques is a seasoned Security and Risk professional, specializing in integrating risk management practices and processes to effectively support decision making with meaningful data while minimizing the overhead and meeting regulatory expectations, and in communicating security and risk to technical and non-technical executive stakeholders. In her current role as a Director of Risk Methodologies at Capital One's Technology Risk Management team, Marta is responsible for defining methodology and practices for risk and controls management, and providing risk intelligence to benchmark risk analysis and monitoring. Her previous experience in the industry ranges from IT audit and risk functions at Deloitte to conducting research in cybersecurity at Barcelona Digital Technology Center and includes defining and implementing an integrated risk management framework as a Director of Enterprise Risk Management at ADP, and building a program to support a single reporting platform that enabled exploration of multiple data sources and provided ADP's executive leadership with visibility and insight into the security and risk program.
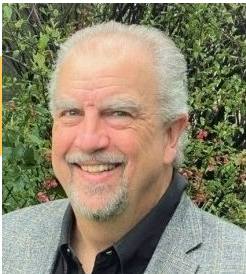
MICHAEL RADIGAN
CYBER RISK ADVISOR, CISCO

WEDNESDAY
2:30 - 3:15 PM

Refining the "R" in GRC at Scale

Mike Radigan has a 22-year career in the cyber security industry where he has focused his professional development efforts on defining and communicating the value cyber security delivers to the business. Mike is recognized as a subject matter expert in the Open FAIR Body of Knowledge and has successfully applied FAIR based cyber risk quantification as a consultant and as the Global FAIR Practice Leader within a Fortune 100 organization. Mike is currently a Cyber Risk Advisor at Cisco where he engages clients on risk-based methods for achieving cost-effective cyber risk management.

SPEAKERS

ANDREW RETRUM
MANAGING DIRECTOR, GLOBAL FINANCIAL SERVICES, SECURITY & PRIVACY, PROTIVITI

Andrew Retrum is a Managing Director and business-oriented leader within Protiviti's Technology Consulting Practice. He currently has dual leadership roles, for both the Global Financial Services Security Practice and the US Security Program & Strategy Practice. Andrew has led Cyber Program Offices for several large institutions as part of broader business transformation efforts. He is an advocate for the adoption of the quantitative and advanced IT Risk measures, currently on the Advisory Board of the FAIR Institute, fostering improved risk management practices across the security landscape.

WEDNESDAY

3:45 - 4:30 PM

Scaling a Quantitative Risk Management Program

NICOLA (NICK) SANNA
PRESIDENT, FAIR INSTITUTE

Nick Sanna founded the FAIR Institute to help advance the discipline of measuring and managing information and operational risk. Under his leadership, this expert non-profit organization has grown to over 13,000 members worldwide and has been recognized as one of the three most influential industry organizations of the last 30 years. Nick is also the CEO of RiskLens, that pioneered the cyber risk quantification software market and sits on the board of the Internet Security Alliance, author of the NACD Cyber Risk Handbook.

SPEAKERS

DAVID SEVERSKI
SENIOR SECURITY DATA SCIENTIST, CYENTIA INSTITUTE

David F. Severski is an information security data scientist, specializing in quantified risk management. He has provided risk management expertise across diverse industries — retail, aerospace, finance, energy, and healthcare. David brings both broad and deep expertise in a number of technical areas with a special focus on cloud technologies and DevOps practices. He strives to combine rigorous methods, technical expertise, and a human-centered approach to advance the state of evidence-based information security risk management. David lives in Worcester, MA with a low-maintenance spouse, a high-maintenance house and a spiffy fedora.

TUESDAY
4:15 - 5:00 PM

Unveiling the IRIS 2022: Bigger Scale, Greater Depth, and More Data for Your CRQ Program

WEDNESDAY
3:45 - 4:30 PM

Scaling a Quantitative Risk Management Program

KRISHNA SHESHABHATTAR
DIRECTOR, SECURITY, RISK, AND COMPLIANCE, EXPEDIA GROUP

Krishna is an experienced governance, risk & compliance (GRC) professional with over 10 years of experience working in risk and audit domains. As a Director of Security Risk and Compliance at Expedia Group, he is responsible for defining the security risk strategy, roadmap and overall maturity in addition to overseeing third-party risk management and cloud security compliance efforts. Krishna worked at Microsoft (treasury function) and PriceWaterHouseCoopers (PwC) (Systems & Process Assurance) prior to Expedia Group. Krishna has an MBA from University of Washington and a master's degree in Information Systems & Decision Sciences (minor in Internal Auditing) from Louisiana State University.

WEDNESDAY
1:45 - 2:30 PM

Expedia Groups' Approach to Build an Effective Security Risk Management Program using FAIR

SPEAKERS

BRYAN SMITH
CTO, RISKLENS

Bryan is the CTO of RiskLens. He is a broad technologist with over 20 years of software engineering experience. His expertise includes building enterprise scale web applications, cyber security, and big data. Bryan led the development of RiskLens' enterprise cyber risk quantification and management platform.

Prior to RiskLens Bryan help build the nation's first digital archives helping it scale 3400% over 5 years. Bryan earned his M.S. in Computer Science and Business Administration as well as his B.S. in Computer Science from Eastern Washington University.

TUESDAY
1:00 - 1:45 PM

How to Scale FAIR Programs with Controls Analytics

RANDY SPUSTA
GLOBAL COMPETENCY LEADER, SECURITY STRATEGY RISK & COMPLIANCE PRACTICE, IBM SECURITY

Randy Spusta is the Global Competency Leader of IBM's Security Strategy Risk & Compliance practice. He manages IBM's offerings for Security Strategy, Risk Quantification, TPRM, GRC and IT Risk Management. He has extensive experience and success in leading client engagements in the areas of enterprise risk management, IT Risk, risk quantification, operational improvement, crisis management, organizational transformation and large program management.

He has also advised Congressional staffers (in the US) on technology trends and Members of Parliament (Australia) on Risk Mitigation strategies. Randy was an advisor to the 2000 Olympics (Sidney, Australia) in crisis management and contingency planning.

WEDNESDAY
1:45 - 2:30 PM

Expedia Groups' Approach to Build an Effective Security Risk Management Program using FAIR

SPEAKERS

DANIEL STONE

ASSOCIATE DIRECTOR, SECURITY & PRIVACY, PROTIVITI

Daniel has 10 years of experience leading a variety of Information Security program and risk assessments, primarily using industry frameworks such as the NIST Cybersecurity Framework. He specializes in Cyber Risk Quantification using the FAIR methodology, and has worked with a variety of clients to analyze cyber risks and implement ongoing risk quantification programs. He holds the Open FAIR Foundation certification, as well as CPA, CISSP, and CISA certifications. Daniel focuses on the Healthcare and Consumer Products / Retail industries, but has experience with a wide variety of industries and their unique Information Security risks.

WEDNESDAY
3:45 - 4:30 PM

CIS, NIST 800-53, ISO27000 - Mapping Leading Control Frameworks to FAIR-CAM™

MATTHEW TOLBERT

SR CYBERSECURITY SPECIALIST, SUPERVISION AND REGULATION, FEDERAL RESERVE BANK OF CLEVELAND

Matt Tolbert is the Senior Risk Specialist for cyber risk management supervision at the Federal Reserve Bank of Cleveland. He regularly contributes to the development of the Federal Reserve's cybersecurity supervision and examination programs, and co-leads the Federal Reserve's Coordinated Cybersecurity Continuous Monitoring (CCCM) program. He recently contributed to the forthcoming update to the FFIEC Information Security Handbook, which provides banking regulators with guidance on assessing the extent of financial institutions' information security risk exposure. His current work involves integrating the Federal Reserve's research on cyber risk and financial stability into large bank supervisory planning.

Mr. Tolbert joined the Federal Reserve in 2018, bringing over 20 years of expertise in cybersecurity operations and technology risk management. He has served as a management consultant with PricewaterhouseCoopers as well as held leadership roles with BNY Mellon, First Niagara Bank, Westinghouse, and the Federal National Mortgage Association. He has also served as an operational risk management expert with the Department of the Treasury's Office of the Comptroller of the Currency (OCC). His experience includes addressing nation-state cyber intrusions, implementing cybersecurity, risk management, and IT audit programs for large organizations, as well as building global security operation centers.

TUESDAY
3:30 - 4:15 PM

Trends in Determining Systemic Cyber Risk for the Financial Services Industry

SPEAKERS

MARK TOMALLO
CHIEF INFORMATION SECURITY OFFICER, VICTORIA'S SECRET

TUESDAY
10:00 - 10:45 AM

Driving Culture Change - From a Compliance to a Risk-based Approach to Cybersecurity

Mark is the Chief Information Security Officer at Victoria's Secret. He has more than 23 years security experience in both Fortune 500 and start-up environments. Mark has founded and sold multiple companies and held Senior Leadership roles at Victoria's Secret / LBrands, Cisco Systems, Cardinal Health, Ascena Retail Group, EasyLink Services. Mark's technology and business experience includes due dilligenceanalysis and integration planning for 51 acquisitions and 7 large divestitures in the technology, health services, intelligence / government and retail industries.

EVAN WHEELER
SR. DIRECTOR, TECHNOLOGY RISK MANAGEMENT, CAPITAL ONE

WEDNESDAY
9:45 - 10:45 AM

Communicating Cyber Risk to the Board and the Business: How Is It Changing?

Evan Wheeler, Senior Director, leads the Risk Identification & Assessment team within Technology Risk Management at Capital One. Evan got his start in cybersecurity working with the U.S. Department of Defense in a Security Operations Center (SOC) and has since held several executive level cybersecurity and operational risk management roles at global organizations such as MUFG Union Bank, Depository Trust & Clearing Corporation (DTCC), and various FinTech firms. At MUFG, Evan designed and implemented a new 2nd Line Information Risk Management program, focusing on harmonizing the tech/cyber assessments with the enterprise risk framework, and deploying a data driven methodology to quantify risk for IT processes.Evan originally joined the DTCC with responsibility for developing a risk framework for the cyber organization, and later moved on to oversee 2nd Line Operational Risk Management for ten diverse lines of business, subsidiaries, and joint ventures. Along the way, he drove major initiatives such as a migration to AWS, implementing DDoS protection, dynamic application security testing, and privileged access control. During his tenure at DTCC, Evan was actively involved with cross-sector initiatives through the FSSCC and FS-ISAC.

SPEAKERS

TIM WYNKOOP
SR. INFORMATION SECURITY RISK ENGINEER, EQUINIX

Tim is a Sr Information Risk Engineer at Equinix. He has his undergraduate degree in International Business from the Ohio State University, and his MBA from Keller Graduate School of Management. He has been in Risk Management for over 15 years, 6 of which has been in risk quantification. Throughout that time, he has had the opportunity to work in a variety of risk disciplines including quantitative & qualitative risk assessments, business continuity & disaster recovery, information and operational risk management and additionally has experience with the 3 lines of defense model. Tim has been part of the FAIR institute since 2016.

WEDNESDAY
3:45 - 4:30 PM

Building a Strong Foundation for your Quantitative Risk Management Program

🐦 /FAIRInstitute

in /company/fair-institute

🏀 fairinstitute.org