GLOBAL RESILIENCE FEDERATION

SUMMIT ON SECURITY & THIRD-PARTY RISK

THURSDAY, OCTOBER 7, 2021

8:45 - 9:00 AM EDT	**OPENING REMARKS**	General Session
9:00 - 10:00 AM EDT	**OPENING KEYNOTE: FUTURE OF THIRD PARTY AND SUPPLY CHAIN SECURITY** *Jonathan Dambrot, Principal, Cyber Security Services, KPMG* *Mitushi Pitti, Director, Cyber Security Services, KPMG* *Mike Wagner, Sr. Director, Global ISRM Leader for Supply Chain, Johnson & Johnson Technology*	General Session
10:00 - 10:15 AM EDT	**COFFEE BREAK**	General Session
10:15 - 11:00 AM EDT CONCURRENT SESSIONS	**AMERICA'S CYBERINSURGENCY** The cybercrime cartels have become dramatically more sophisticated in 2021. This presentation will highlight significant shifts in the modern kill chain. Adversaries are now expanding upon their core capabilities with more modular and extensive malware, allowing for more diversity in their overall operations and becoming much more brazen as a result, shifting tradecraft towards more destructive attacks combined with outright sale of direct access into corporate networks. Burglary has escalated to home invasion as "island hopping" abounds. These are just a few of the trends related to cybercrime cartels, many of which are treated as national assets. Kellermann will depict the threat actors' latest techniques, tips for defending against them, and what to expect as these actors continue to evolve. The presentation will highlight a proactive defensive paradigm named Intrusion Suppression to mitigate cyber escalation. *Tom Kellermann, Member, U.S. Secret Service Cyber Investigations Advisory Board*	Breakout #1
	REFLECTIONS ON NAVIGATING A CLOUD JOURNEY Genpact, a professional services firm with over 90,000 employees, has been on a multi-year journey of adopting cloud across SaaS and IaaS. They have been early adopters of solutions like CASB and Cloud Security Monitoring. Join them in this session to hear them share lessons learnt in their journey, and a practitioner perspective in deploying best practices. *Ram Hegde, CISO, Genpact* *Swatantr Pal, Incident Response & Information Protection Leader, Genpact* *Rohit Kohli, Cloud Security Leader, Genpact*	Breakout #2
11:15 - 11:45 AM EDT CONCURRENT SESSIONS	**MEASURING THE IMPACT OF SUPPLY CHAIN RISK** Organizations of all shapes and sizes are critically dependent on complex supply chains. Traditional methods of managing third-party risk simply do not provide the timely, accurate information necessary to scale at business speed. To gain complete visibility into threats coming from your digital supply chain, you need a holistic view that provides you with real-time, actionable intelligence that allows you to focus on the risk that matters most to your business. Attendees will learn: How recent supply chain events have shifted the mindset of executives and board members; What data points are critical to measuring the effectiveness of a supply chain risk management; The methods that the most well-built third-party risk programs are utilizing to combat supply chain threats. *Jonathan Ehret, CISSP, CISA, CRISC, Vice President, Strategy & Risk, RiskRecon*	Breakout #1

**Agenda subject to change.*

11:15 - 11:45 AM EDT CONCURRENT SESSIONS	**MATURING SECURITY OPERATIONS IN A REMOTE WORLD** In the past two years, the world rapidly transitioned from physical work to remote and hybrid environments. The shift was inevitable, but as organizations continue to catch up, security operations need effective strategies and solutions for meeting these new requirements. In the past, fusion centers enabled law enforcement, military, and security teams to reach their full potential by unifying people, processes, and technology under one roof; and today, cyber fusion centers are doing the same but with both cloud infrastructure and remote teams as a primary element. By tapping into emerging technologies like AI and machine learning, augmenting existing security tools and consolidating them, and bringing humans up to machine speed, cyber fusion centers are becoming the future of security operations. During this brief chat, we'll offer a primer on how and why a cyber fusion center is the future of the SOC. Key Takeaways: 1. Why and how SOCs unify their people, processes, and technology 2. Finding a balance between human intelligence and machine speed/automation 3. Using a data-driven approach to threat intelligence *Neal Dennis, Threat Intelligence Specialist, Cyware; Colin Blumer, Integrations Manager, Cyware*	Breakout #2
12:00 - 12:30 PM EDT CONCURRENT SESSIONS	**RECALIBRATION - RETURNING TO NORMALCY WITH YOUR THIRD PARTY ASSESSMENT PROGRAM** As normalcy returns, there is a tendency to go back to the way things used to be. In this session, we will cover the adjustments that organizations have made in the assessment process as they and their vendors pivot between their original business environment, to a work from home environment, and then back again. Third party risk management programs are frequently scrutinized for value and returning to onsite assessments is just one of the efforts under the microscope. Along with newly streamlined assessment efforts such as continuous monitoring and partnerships with other 2LD organizations, we will share with attendees what our members and research have advised us of the common success and challenges for the current environment. As we return to normalcy, it's important to be fluid in your efforts as being flexible is now too rigid. *Tom Garrubba, Vice President, Shared Assessments*	Breakout #1
	DIGITAL SUPPLY CHAIN THREATS – PREVENT VULNERABILITIES IN YOUR SOFTWARE Software is eating the world is a common refrain describing the oversized influence software has in how we run our businesses. From WFH initiatives, digital transformation to application development demands, third party software usage is on the rise. A recent study has shown that 100% of the most popular software contains highly vulnerable components. The challenge is how do you proactively uncover, manage and reduce the inherent risk that this code introduces. New products have emerged which prevent this risk by analyzing this COTS or 3rd party code, for vulnerabilities while creating a SBOM (software bill of materials). *Vince Arneja, Chief Product Officer, GrammaTech*	Breakout #2
12:45 - 1:15 PM EDT	**LUNCH KEYNOTE: MANAGING CYBER RISK ACROSS THE EXTENDED VENDOR ECOSYSTEM** During this session, Jim Rosenthal, BlueVoyant co-founder and CEO, will share the key insights and findings from our BlueVoyant 2021 Global Insights Report. The BlueVoyant 2020 Global Insights Report stated that "managing third-party vendor cyber risk is fast becoming the defining cybersecurity challenge of our time." This year, the survey not only explores the scale of the challenge; but also the level of supply chain breaches and the resources risk executives have at their disposal. Join this session to hear what your peers in multiple industries and regions shared about their response to the challenges of ensuring cybersecurity in their supply chain and our recommendations on how to manage and protect your ecosystem. *Jim Rosenthal, Co-Founder and CEO, BlueVoyant*	General Session

**Agenda subject to change.*

1:15 - 1:30 PM EDT	**CYBER SUPPLY CHAIN RISK MANAGEMENT: THERE IS HOPE... AND HELP!** Cyber Supply Chain Risk Management, or C-SCRM, has undoubtedly come to the forefront of the news cycle in the cyber world due to unprecedented breaches like the SolarWinds and Colonial Pipeline hacks. So, it's no surprise C-SCRM has also become the one of the primary concerns of company executives across the world, and cyber and compliance teams are being asked to implement C-SCRM into their cybersecurity risk management plans. Fortunately, there are free and authoritative resources available to those struggling to get a foothold on where to start. In this session, Vincent Scheivert, Director of Technical Strategy for Telos Corporation, will discuss why implementing a C-SCRM plan is critical, what the challenges are, and the guidance you can find in resources from the National Institute of Standards and Technology (NIST) and the ICT Supply Chain Risk Management (SCRM) Task Force established by CISA. *Vincent Scheivert, Director of Technical Strategy, Telos*	General Session
1:45 - 2:30 PM EDT CONCURRENT SESSIONS	**EFFECTIVE THIRD-PARTY RISK MANAGEMENT** This session will help companies build and/or maintain a third-party risk management function given the sweeping changes in technology, regulatory guidance and risk management practices. An end-to-end view of the third-party risk management function will be discussed. There is no cookie-cutter approach as each solution requires customization to the company. *Greg Gist, Director of Cyber, Cloud and Operational Risk, Promontory Financial Group*	Breakout #1
	SUPPLY CHAIN SECURITY: WHERE THE GLOBAL POLICYMAKING COMMUNITY IS HEADING In the wake of the COVID-19 pandemic, businesses began re-examining their supply chains. Relatedly, nations around the world began re-examining their bilateral relationship with China - policymakers took a hard look at the national and economic security risk of reliance on untrustworthy partners for critical components in key industries and technologies such as telecommunications infrastructure, semiconductors, software applications, cameras, drones, computers and mobile devices. And they are considering industrial policy to support the domestic capacity of these and related industries. This session will provide an overview of those supply chain security efforts in global capitals, and where things go from here. *Andy Keiser, Principal, Navigators Global*	Breakout #2
2:45 - 3:30 PM EDT CONCURRENT SESSIONS	**REGULATORY DEVELOPMENTS AND THE IMPACT ON THIRD PARTY RISK MANAGEMENT** Regulatory compliance has been a stable item on many board agendas but lately it has been the number one topic within organizations. There are a variety of reasons behind this focus but the main drivers are related to the threat landscape growing in complexity, momentum of digital transformation, political and social unrest, as well as a global pandemic. But what does this mean from a third party risk perspective? In this session we will explore regulations that you need to be aware of, as well as how to incorporate regulatory compliance reviews into your third party risk assessments. We will also discuss why you should be ensuring your third parties have strong regulatory compliance controls in place and the impact it could have on your organization if they do not. *Julie Gaiaschi, CEO & Co-Founder, Third Party Risk Association*	Breakout #1

*Agenda subject to change.

2:45 - 3:30 PM EDT CONCURRENT SESSIONS	**RESPONSE TO RANSOMWARE – OPERATIONAL RESILIENCE** Join this session to learn about the cross-sector work of security industry leaders who are developing a framework to help ensure resilience in the face of destructive malware, ensuring the immutable and recoverable nature of data, systems, networks, applications and configurations. There is a lot of discussion of data backups in the face of cyber attacks, but we must also have the ability to maintain operational continuity in the face of an attack. Safe data doesn't mean much if you or your customers can't access it. The Operational Resilience Framework (ORF) Working Group is seeking to address both problems. *Trey Maust, Chair, Operational Resilience Framework Work Group & Executive Chairman, Lewis & Clark Bank*	Breakout #2
3:45 - 4:30 PM EDT CONCURRENT SESSIONS	**EXPLAIN TO ME WHAT YOU MEAN BY BUSINESS RISK – BUILDING A THREAT INTELLIGENCE FUNCTION FOR THE OPERATIONAL RESILIENCE ERA** Forward-leaning approach to managing risks. This is how one should think of threat intelligence these days, no longer as a technical niche function that sits in the back of the room and passively collects indicators of compromise. Intelligence should be used to challenge conventional wisdom about what your senior leadership should be concerned about. Intelligence teams should make senior leadership and business stakeholders feel 'uncomfortable' about how they think about certain scenarios or the state of their organization's risk posture. This presentation explores how to fully operationalize and evolve your intelligence program in light of the growing regulatory and organizational focus on operational resilience. In this context, a holistic approach to intelligence is one that goes past structural silos, allowing organizations to anticipate, and prepare for, any type of operational disruption to the business. It will also discuss how to measure the value of your intelligence function. *Valentina Soria, Executive Director, Head of Global Intelligence, Morgan Stanley*	Breakout #1
	CONSEQUENCE DRIVEN RESILIENCE: UTILITY PERSPECTIVES ON ACCOMMODATING CYBER, CLIMATE AND SYSTEMIC RISK Organizations of all shapes and sizes, including electric utilities and their stakeholders, are wrestling with the proper balance of consequence, likelihood, and prioritization in the face of an increasing array of risks and threats, whether natural or manmade, which can come at any time and in combination. In a fireside chat format, Sam Rozenberg and Andy Bochman will discuss how organizations large and small are seeking this balance while approaching resilience challenges by examining current case studies that show the importance of a risk-based approach to resilience. *Andrew Bochman, Senior Grid Strategist, Idaho National Laboratory* *Sam Rozenberg, Director, Security Risk Analysis, KPMG*	Breakout #2
4:30 PM EDT	**DAY ONE CONCLUDES**	

**Agenda subject to change.*

FRIDAY, OCTOBER 8, 2021

9:00 - 9:15 AM EDT	**OPENING REMARKS**	General Session
9:15 - 9:30 AM EDT	**COFFEE BREAK**	General Session
9:30 - 10:15 AM EDT CONCURRENT SESSIONS	**ARE YOUR VENDORS YOUR WEAKEST LINK?** Understanding third party vendor risk is essential for organizational resiliency. This session will address best practices for assessing vendor risk and resiliency, understanding inherent risks and potential impacts to the organization, and tying vendor risk into a comprehensive resiliency program. *Michelle Cross, Vice President, Business Continuity Center of Excellence, Fidelity* *Alison Tarnopol, Director, Business Continuity, Fidelity Investments*	Breakout #1
	METHODOLOGY FOR ACTIONABLE, EFFECTIVE THREAT INTEL COMBINING ALL ASPECTS INTELLIGENCE FOR SUCCESS FROM A MEDICAL DEVICE MANUFACTURER During this presentation attendees will receive firsthand field experience-based lessons for building an effective cyber threat intelligence program, combining all aspects of cyber threat intelligence, OSINT, SOCMINT, HUMINT, SIGNINT, etc to respond to asymmetric threats confidently. Discussed items include challenges, issues and actionable capabilities in building a CTI program and future proofing your manufacturing capability from the unknown vagaries of vulnerability disclosures. *William Hagestad, Cyber Threat Intelligence Analyst, Medtronic*	Breakout #2
10:30 - 11:15 AM EDT CONCURRENT SESSIONS	**VALUE FROM ENTERPRISE CYBER RISK ASSESSMENT** Given the critical nature of cyber security to the overall functioning of an organization, Financial Services Organizations (FSOs) are starting to measure and manage cyber risk as one of the critical risks in their overall risk portfolio. While FSOs are starting to gain an understanding of their cyber risk across the entire business franchise, understanding the cyber risk landscape at an individual Line of Business (LOB) level has remained elusive. The DTCC Enterprise Cyber Risk Assessment (ECRA) enables each LOB to understand the cyber security risk portfolio that pertains to each LOB. The methodology for identifying LOB cyber risks includes analyzing prior cyber risk assessments, incidents, and issues and threats across the enterprise and deriving the LOB specific view based on the business context, threat landscape, and technology footprint. The approach includes a bottoms up analysis of data, and a top down validation of the risks with the LOB. Once cyber risks are included in the business risk portfolio, LOBs are able to extend their existing business and operational risk management practices to cyber risk management, and take a holistic risk management approach across the entire risk portfolio. *Ajoy Kumar, Head of Cyber/Tech Risk, DTCC*	Breakout #1
	RANSOMWARE READINESS: WHAT NOT TO DO Chris and Allan share horror stories about organizations that have made terrible mistakes in defending against, and recovering from, ransomware attacks. (We won't name and shame!) We hope to get the audience laughing at the foolishness, but to also reflect on how their ransomware readiness could be improved. *Allan Alford, CISO & CTO, TrustMAPP* *Chris Richter, North America Security Practice Leader, Avanade*	Breakout #2

**Agenda subject to change.*

SUMMIT ON SECURITY & THIRD-PARTY RISK

	MATURING A STARTUP SECURITY PROGRAM Doug Levin, executive director of K12 SIX, takes lessons learned in the heavily attacked and under-resourced education sector and offers them for implementation in new or growing security programs, in any Industry. What are the first steps a company should take to protect itself? What are the foundational cybersecurity elements that all companies should have in place? Attend to learn more! *Doug Levin, National Director, K12 SIX*	Breakout #1
11:30 AM - 12:15 PM EDT CONCURRENT SESSIONS	**VERIS A4 THREAT MODELING** VERIS, the Vocabulary for Event Recording and Incident Sharing, is a set of metrics designed to provide a common language for describing cybersecurity incidents (and data breaches) in a structured and repeatable manner. VERIS provides cyber defenders and intelligence practitioners with the ability to collect and share useful incident-related information - anonymously and responsibly – with others. VERIS underpins the annual Data Breach Investigations Report. VERIS and its A4 Threat Model – Actors, Actions, Assets, Attributes – help codify incident-related information for threat modeling, intelligence analysis, breach mitigation, and detection / response improvement. Key takeaways for this session include: ▪ Understanding cybersecurity incidents through the VERIS lens ▪ Recognizing the VERIS A4 Threat Model: Actors, Actions, Assets, Attributes ▪ Getting started in Threat Modeling with VERIS *John Grim, Head of Research, Development, & Innovation, Verizon Threat Research Advisory Center*	Breakout #2
12:15 PM EDT	**SUMMIT CONCLUDES**	

**Agenda subject to change.*