GLOBAL RESILIENCE FEDERATION

2022 SUMMIT

SECURITY & THIRD-PARTY RISK

October 27-28

WEDNESDAY, OCTOBER 26, 2022

		Room
6:30 - 8:30 PM EDT	WELCOME RECEPTION	*POSE Lounge*

THURSDAY, OCTOBER 27, 2022

		Room
7:30 - 8:30 AM EDT	BREAKFAST	*Riverview AB*
8:30 - 9:00 AM EDT	OPENING REMARKS FROM GRF CHAIRMAN BILL NELSON AND CEO MARK ORSI	*Riverview AB*
9:00 - 10:00 AM EDT	OPENING KEYNOTE *Dan Menicucci, Chief Security Advisor, Microsoft Security*	*Riverview AB*
10:00 - 10:15 AM EDT	MORNING COFFEE AND TRANSITION BREAK	*Riverview 4&5*
10:15 - 11:00 AM EDT CONCURRENT SESSIONS	ADVANCED MONITORING Looking back at some of the most sophisticated attacks experienced over the past couple of years, organizations have grappled with tuning their preventative controls in an attempt to get ahead of advanced persistent threats. Monitoring for compromised vendors, living off the land and Ransomware activity has grown into its only cyber-discipline. What are the most important technologies, tools and tactics you should build in your program? How do you avoid alert fatigue? These are topics we'll explore to enhance your detection capabilities or make the case for the tools you'll need to get there. *Kyle Salous, AmLaw 200 Law Firm*	*Riverview 1*
	ENCOURAGING CONSISTENT THIRD-PARTY SECURITY PROTOCOLS: A PRACTICAL FRAMEWORK This session will showcase the current challenges and opportunities for practitioners in managing their third-party vendor ecosystem. Representatives from major consumer packaged goods organizations will participate in a roundtable discussion focused on each specific stage of the vendor lifecycle, from procurement to offboarding, to determine where collaboration amongst industry can better facilitate secure third-party procedures. For shared challenges, the group will look to identify collective best practices, as well as novel approaches to better address the issues at hand. *Mark Wehrle, Campbell Soup Company; Chris van Schijndel, J&J; Bryan Hubbard, Mars; Mitushi Pitti, KPMG; moderated by Kristy Hornland, KPMG*	*Riverview 2*
	OPERATIONAL RESILIENCE TABLETOP – WHEN CRITICAL ASSETS LIVE IN THE CLOUD Cloud services have become an integral part of nearly every business strategy. As organizations leverage the agility and efficiency of cloud-based solutions to host business critical workloads and data, cloud service providers get better and better at providing reliable and resilient solutions. But how much faith can you really put in a cloud based solution, even when the provider has a strong security program and many layers of security and redundancy? Referencing rules in the new GRF Operational Resilience Framework, Jon Washburn will lead attendees through Stoel Rives' assessment of risk to its document management ("DMS") cloud and what led the organization to engineer a separate, immutable backup of this 20+TB information store - despite strong assurance from the cloud service provider. The session will then move through a tabletop scenario designed to highlight when the organization may be placing too many critical assets in one basket – even when that basket seems 'bullet-proof,' and end with Q&A. *Jon Washburn, Stoel Rives LLP*	*Riverview 3*
11:00 - 11:15 AM EDT	TRANSITION BREAK	

11:15 - 11:45 AM EDT	**RANSOMWARE DUMPS SITES: ONGOING CHALLENGES OF EVALUATING YOUR EXPOSURE** Ransomware dumps sites are an ongoing issue for organizations. The advent of double-extortion has increased victims' willingness to pay, or risk their information appearing on ransomware dump sites. Due to the interconnected nature of business operations, these dumps can include sensitive information from third parties. Issues in accessing and downloading the data can affect companies ability to accurately mitigate these risks. In this presentation, we will evaluate some of the ongoing challenges associated with the exposure from ransomware leaks. *Ian Gray, Flashpoint*	*Riverview 2*
	THIRD-PARTY RISK DEEP DIVE: CALCULATING INHERENT RISK When building an efficient vendor risk management program, it is critical to prioritize which vendors present the most risk. Knowledge of your third parties' inherent risks can help increase security and performance and change the way you run your vendor risk management program. In addition, by understanding where to prioritize your time, you can invest resources in assessing and monitoring the third parties that matter most to your business. In this webinar, you'll learn how to: • Develop inherent risk calculations and a scoring methodology • Tier your third parties by criticality and high risk • Scope and schedule vendor assessments based on inherent risk scores. *Ed Thomas, ProcessUnity*	*Riverview 3*
11:45 - 12:00 PM EDT	**TRANSITION BREAK**	
12:00 - 12:30 PM EDT	**CLOUD MIGRATION - CYBERSECURITY SUCCESS** What is Cybersecurity Success, and how can you apply that to your Cloud environments? Marco DiPasquale of Cipher and Jacob Eggemeyer of LogRhythm will introduce you to why our partnership is positioned to achieve success. Knowing your motivations for Cloud migration and use and Cybersecurity, regardless the platforms you choose, and the importance of collaborative design, along with 3 critical ingredients and questions you should ask yourself will be presented, leading to a cyber maturity discussion and summary information. *Marco Di Pasquale, Cipher; Jacob Eggemeyer, LogRhythm*	*Riverview 2*
	OPERATIONALIZING SUPPLY CHAIN DEFENSE FROM FINDINGS TO MITIGATION The evolution of supply chain cyber risk management has taken us from self-attestation questionnaires to security ratings services and advanced artificial intelligence (AI) technology. Along the way, organizations have acknowledged that extended supply chain ecosystems are a favorite attack vector, necessitating the need for comprehensive and continuous visibility across all of their suppliers. Now on the cusp of achieving operational efficiencies and true supply chain cyber defense, organizations are realizing that automated technology solutions need to be complimented with analyst-backed curation and validation in order to enable teams to prioritize supplier risk for rapid and direct remediation. How does your organization get there? Like many organizations, your maturity level may not be where you'd like it to be. You may still be relying on point-in-time questionnaires or be experiencing the frustration of too many false positive alerts and not enough staff to prioritize what's really important. In this session, you'll hear about how combining AI technology and human investigations may comprise the next step in your evolution to operationalizing supply chain cyber risk management. *Mark Risoldi, BlueVoyant*	*Riverview 3*

12:30 - 12:45 PM EDT	**TRANSITION BREAK**	
12:45 - 1:45 PM EDT	**LUNCH AND KEYNOTE FROM CYBERVADIS & ONETRUST** *Edouard Lacarriere, Cybervadis; Chris Paterson, OneTrust; Andrew Moyad, Shared Assessments; moderated by Jonathan Dambrot, KPMG*	*Riverview AB*
1:45 - 2:00 PM EDT	**TRANSITION BREAK**	
2:00 - 2:45 PM EDT CONCURRENT SESSIONS	**COLONIAL PIPELINE, UKRAINE, AND TAIWAN: HOW C-SUITE EXECUTIVES OUGHT TO THINK ABOUT THE THREAT OF CYBER COLLATERAL DAMAGE AND DESTRUCTIVE CYBER ATTACKS IN THE MODERN ERA** In light of the recent Russian invasion of Ukraine and the potential threat of a Chinese invasion of Taiwan in the not-so-distant future, CSuite executives must increasingly consider the potential risk posed by cyber attacks that are either designed to create destructive effects against their organization or which may result in collateral damage to their organization even where they are not the intended target. This session will look at the historical lessons of cyber attacks like Colonial Pipeline, JBS, NotPetya, Sony Pictures, and Las Vegas Sands, as well as recent trends in geopolitics and cyber offensive operations to help senior business executives think about and plan for threats to their operational and business infrastructure. The session will provide tools and frameworks for the assessment of cyber geopolitical risk in private sector boardrooms and executive offices. *Jamil Jaffer, National Security Institute at George Mason University's Antonin Scalia Law School*	*Riverview 1*
	SECURING AMERICA'S MANUFACTURERS: EVOLUTION OF CYBERTHREATS IN THE 21ST CENTURY Attend this session to learn more about past, present and future threats to U.S. manufacturing through the lens of speakers representing healthcare, energy and public/private security partnerships. Speakers have extensive experience in securing different aspects of critical infrastructure, and all have witnessed a change in approach from threat actors as technology, nation-state requirements, ransom landscape, and individual sophistication have adapted to the times, and the targets. *Michael Mylrea, Resilience; Zach Tudor, Idaho National Laboratory; moderated by Tim Chase, Manufacturing ISAC*	*Riverview 2*
	MEASURING PERFORMANCE OF A SECURITY PROGRAM THROUGH MATURITY MODELS Whether your company has a mature security program or you are just beginning your journey, let's take a look through the inception, maturation and maintenance of the ICSP (Information and Cyber Security Program) at Otter Tail Corporation. This session will showcase how to map progress through maturity models and industry performance metrics and use results to target priorities, mature capabilities, and increase return on investments. *Don Redden, Otter Tail Corporation*	*Riverview 3*

2:45 - 3:00 PM EDT	TRANSITION BREAK	
3:00 - 3:45 PM EDT CONCURRENT SESSIONS	**BUILDING VS. MATURING A THIRD-PARTY RISK PROGRAM** Initial build out of Third Party Risk Management (TPRM) poses a different set of challenges when compared to enhancement of a program in a mature state. During this session we will dive into different approaches firms can adopt to maximize and expedite value proposition to the organization, tailored to the different maturity levels of a third-party risk program. Whether it's initial determination of people, process and technology or modeling of concentration and vulnerabilities, stakeholder buy in is key to the operational effectiveness and sustainability of the TPRM. This session is dedicated to lessons learned and best industry practice for building and maturing third-party risk programs within your organizations. *Olga Voytenko, Silicon Valley Bank*	*Riverview 1*
	CYBER RISK INSURANCE TRENDS "Cybersecurity insurance is too expensive. Coverage is too narrow in scope. It'll never pay out. I'm held to too high a defensive bar to meet coverage requirements. We have data backups so we won't pay a ransom anyway." Join this session to uncover misconceptions, learn how to prepare your organization and how to guard yourself in a rapidly evolving marketplace. Explore insurance risk management with a panel featuring an incident response practitioner, a broker, an attorney and an underwriting consultant. *Jeffrey Shaffer, Stroz Friedberg; Nick Jennings, AON; Shawn Tuma, Spencer Fane LLP; Sean Scranton, WTW; moderated by Mark Orsi, Global Resilience Federation*	*Riverview 2*
	BENCHMARK YOUR SECURITY Your security is defined by the threat: from prevention that is left of boom to the speed with which you can detect, respond, and recover from a breach. Structural awareness consists of identification (what you have) and protection along with your exposure to third parties and your own development process (CI/CD pipeline). Operational awareness covers post-deployment (it's been thrown over the proverbial wall) phases of what we can control and understand post-incident. We will discuss beyond CIS controls as a benchmark in both pre/post operational environments to follow Dan Geer's philosophy that "the truth is best achieved by adversarial procedures." When it comes to compromises the adversary gets the only vote that really counts. *Bryson Bort, SCYTHE*	*Riverview 3*
3:45 - 4:00 PM EDT	TRANSITION BREAK	

4:00 - 4:45 PM EDT CONCURRENT SESSIONS	**SEMICONDUCTOR SUPPLY CHAIN SECURITY CONSIDERATIONS** This presentation will provide an overview of semiconductor development phases and their associated threats when using third party tools, third party fabs and third party IPs. After understanding the threat landscape we will explore potential directions for mitigations, future standards and methods. *Jean-Philippe Martin, Intel*	*Riverview 1*
	TECTONIC SHIFTS IN SUPPLY CHAIN MANAGEMENT For the past several decades global enterprises have been diligent in their effort to optimize supply chain logistics and significantly reduced the amount of product inventory paid for while improving time to market for consumers. Several disruptive categories of events have jolted global enterprises to rethink this approach to supply chain management including: • the global pandemic of COVID-19 • the war in Ukraine and aggressive posture of Russia toward the west • an increasing number of extreme weather events causing business disruption, large population migration and famine due to water shortages • social responsibilities and accountabilities • malicious and destructive software in the global software supply chain *Jim Routh, formerly of CVS Health & MassMutual; Atul Vashistha, Supply Wisdom; Michelle Clement, AWS*	*Riverview 2*
	FINDING OPPORTUNITIES FOR THE ADVERSARY Having an adversary focused approach to cybersecurity will assist organizations with shaping the malicious actor's behavior, denying them benefits, and pressing costs on their efforts to successfully breach your company. Attendees will come away from this session thinking like an attacker, understanding the risk, and knowing how to leverage critical threat intelligence nodes to gain an edge in defeating cyber adversaries. As threats continue to be more complicated and severe, organizations need to make themselves not just a more hardened target, but a fiercer target causing attackers to seek gains somewhere else. *Brian Hansen, Mastercard*	*Riverview 3*
4:45 - 5:00 PM EDT	**TRANSITION BREAK**	
5:00 - 6:00 PM EDT	**SPONSOR AREA HAPPY HOUR**	*Riverview 4&5*
6:00 - 6:30 PM EDT	**TRANSITION BREAK**	
6:30 - 8:30 PM EDT	**RISKRECON RECEPTION IN THE ATRIUM**	*Lower Atrium*

FRIDAY, OCTOBER 28, 2022

8:00 - 9:00 AM EDT	BREAKFAST	*Riverview AB*
8:45 - 9:30 AM EDT	**A PERFECT STORM 50 YEARS IN THE MAKING: WHY AUTHENTICATION IS BROKEN AND WHAT IT'S GOING TO TAKE TO FIX IT** Despite the oft-quoted statistic that 80% of all security breaches are related to passwords, the situation is actually getting worse with traditional MFA solutions already being bypassed at scale. HYPR CEO, CTO and one-time hacker Bojan Simic describes how attacks take place today and provides a vision for how authentication needs to evolve to address the changing nature of security at every point in the enterprise, consumer and even IoT lifecycle. *Bojan Simic, HYPR*	*Riverview AB*
9:30 - 9:35 AM EDT	TRANSITION BREAK	
9:35 - 10:20 AM EDT CONCURRENT SESSIONS	**BUILDING A SUSTAINABLE ENTERPRISE WIDE CORPRATE RISK POSTURE FROM THE BOARD TO THE CSUITE** This session will detail the core foundations of building and sustaining a comprehensive enterprise wide security posture which descends from leadership through the entire enterprise. Such a posture uses intelligence based metrics, current threat identification, and repeatable business practices to ensure both sustainability and growth in protecting your brand and what you make and sell. Key focus areas will be crisis mitigation, ransomware and third party data storage and vulnerability. *William Evanina, The Evanina Group, LLC*	*Riverview 2*
	OPERATIONAL RESILIENCE FRAMEWORK PANEL In 2021, GRF's Business Resilience Council (BRC) launched a multi-sector working group to develop the Operational Resilience Framework which was released in October 2022. In this session, panelists will review with the audience the design and application of the framework, and describe how it supports rapid recovery of critical services to customers in the face of destructive attacks and adverse events. *Mark Orsi, Global Resilience Federation; Charles Blauner, Team8; Jon Washburn, Stoel Rives, LLP; Trey Maust, Lewis & Clark Bancorp; Susan Rogers, Sumitomo Mitsui Banking Corporation*	*Riverview 3*
10:20 - 10:25 AM EDT	TRANSITION BREAK	
10:25 - 10:55 AM EDT	**RISKS OF DIGITAL EXPOSURE IN MANUFACTURING AND CRITICAL INFRASTRUCTURE SECTORS** A recent study by Cyber Intel Matrix provides a sectoral overview of typical vulnerabilities, weaknesses, and possible future threats in manufacturing. The study found a complex and vertically large network infrastructure in each manufacturing company under scope, a large portion of which contained unmaintained legacy services. Every network examined in the study is filled with vulnerable points. The network infrastructure of manufacturing companies relies on a large number of third-party maintainers, contractors, and developers and software. The amount of potential exposure menacingly increases with the size of this infrastructure. Companies are seemingly trying to adopt state-of-the-art and secure cloud-based solutions and data management, while neglecting their parallel legacy frameworks, which run on outdated and vulnerable software (and firmware). Critical IoT and IIoT remains vulnerable and exposed in many cases. *Andras Patkai, Axalton Group*	*Riverview 3*

10:55 - 11:00 AM EDT	**TRANSITION BREAK**	
11:00 - 11:45 AM EDT CONCURRENT SESSIONS	**THIRD-PARTY RISK: REACTIVE TO PREDICTIVE** It is not a question of if, but when your third-parties will have an incident or breach, causing disruption to your own operations. Learn how to take a risk-based approach to your vendor resilience to ensure that their incidents or breaches do not affect your organization's ability to continue operations. *Greg Rasner, Truist*	*Riverview 2*
	EMERGING SECURITY THREATS AND INDUSTRYWIDE DISRUPTION: CYBERSECURITY LEADERS WEIGH IN ON THE NEED FOR RESILIENCY AND COOPERATION This session aims to provide a strategic view of the challenge in securing the supply chain from the perspective of cybersecurity leaders at major consumer packaged goods organizations. Insights on the broadening and ever-changing supply chain threat landscape will be captured through questions posed to each of the participants. The panel goals are to determine how organizations prepare for and respond to unpredictable disruptions that threaten business continuity and system security. *Martin Bally, Campbell Soup Company; Bill Dzmelyk, Mars; Chris van Schijndel, J&J; moderated by Jonathan Dambrot, KPMG*	*Riverview 3*
11:45 - 11:50 AM EDT	**TRANSITION BREAK**	
11:50 - 12:35 PM EDT	**OT RISK MANAGEMENT - LESSONS LEARNT FROM THE COMMUNITY** With the increasing industrial automation brought about by Industry 4.0, there will be greater connectivity between systems (internal and external). Operational Technology is a growing concern for many asset owners and operators. The talk will look at the drivers, challenges and enablers for securing OT assets. *John Lee, OT-ISAC*	*Riverview 3*
12:35 - 1:35 PM EDT	**LUNCH**	*Riverview AB*
1:35 PM EDT	**CONFERENCE CONCLUDES**	