GLOBAL RESILIENCE FEDERATION

July 2023 Newsletter

TLP CLEAR

## IN THIS ISSUE: LS-ISAO Workshop, AI Guide & MFG Ransomware

**LS-ISAO Chicago Member Workshop**
Join LS-ISAO for the Chicago Member Workshop on July 13! The day will begin with a TLP: RED members-only discussion, followed by presentations covering TTPs of creative breaches, and insights into the responsibilities and actions to be taken by legal and IT in the event of a data security incident. Stick around after the talks to network with your peers at the happy hour. The workshop will be hosted by Dentons. Register here

**Practitioners' Guide to Managing AI Security**
Recognizing the disconnect between AI innovation and AI security, GRF convened a working group with KPMG to facilitate discussions among AI and security practitioners from more than 20 leading companies, think tanks, academic institutions, and industry organizations. The output of this months-long project is the Practitioners' Guide to Managing AI Security. The guide provides considerations to strengthen collaboration between data scientists and security teams across five tactical areas: Securing AI, Risk & Compliance, Policy & Governance, an AI Bill of Materials, and Trust & Ethics. Download

**Manufacturing at Risk: The Growing Threat of Ransomware**
In this webinar, leaders from Manufacturing ISAC, Dragos, and OT-CERT discussed ransomware targeting manufacturing, cybersecurity maturity in the manufacturing supply chain, and dived into victimology, trends and insights for the sector. Panelists also covered available education, training and self-assessments, as well as collective defense opportunities. Register to watch the recording

**The AI Security Balancing Act: Determining the Sweet Spot Between ROI and Risk**
Complementing the recently released Practitioners' Guide, this webinar showcased the current challenges and opportunities in securing Artificial Intelligence in an organization. A multi-sector group of leaders from Wells Fargo, Kenvue, Johnson & Johnson, MITRE, and KPMG discussed insights identified in five critical areas during a months-long AI working group. From defining what AI security means for organizations, to tactical areas of risk & compliance, policy & governance, an AI Bill of Materials, and trust & ethics, the group covered collective better practices, as well as approaches to address AI security governance. Register to watch the recording

**ORF Payments System Exercise**
A draft operational resilience exercise is being developed by the Business Resilience Council's Operational Resilience Framework Working Group. The tabletop exercise will be focused on a wiperware attack against Automated Clearing House (ACH) operations of banks and credit unions, and efforts to restore minimal viable service levels for origination and receipt of ACH payments. Nacha, the rule making body for the ACH Network, is contributing to this initiative, and the intent is to finalize the exercise this summer for release in September among members of GRF, Nacha, and other banking associations. Future plans include ORF exercises for OT/ICS operations that could impact other critical infrastructures.

Interested in becoming a member, sponsor, or partner? Contact info@grf.org.

# K12 SIX & CISA, New Board Member, Final Call for Speakers

**K12 SIX Director Meets CISA Colleagues**
K12 SIX National Director Doug Levin recently met with CISA Director Jen Easterly and a multi-sector mix of colleagues on CISA's Cybersecurity Advisory Committee. In March, Levin began a two year term on the committee to advocate for the unique cybersecurity needs of K-12 education.

**OT-ISAC Managing Director John Lee Talks with Govware**
In a recent discussion with Govware, Lee said that the concept of OT security is relatively new and not well understood. "Equipment makers or the system integrator that installs these [Internet of Things] systems for asset owners and operators often don't have the concept of OT security as it was not needed in the past." Specifically, OT systems makers may lack the technical know-how to adequately secure them from cyberattacks. Part of the challenge could be attributed to the widespread use of commercial-off-the-shelf (COTS) components, said Lee. Read the article

**Siemens Energy VP Joins GRF Board**
Leo Simonovich currently serves as Siemens Energy's Vice President and Global Head of Industrial Cyber and Digital Security, leading the company's industrial cybersecurity line of work. Simonovich brings expertise in cybersecurity of operating technologies to GRF at a time when many sectors are investing heavily in digitizing physical production processes with information technology systems, an approach often called an industrial Internet of Things. Read more

**Get to Know K12 SIX**
Join the K12 Security Information eXchange (K12 SIX) for an overview of work, membership benefits, forthcoming products and events. Since 2016, there have been more than 1,600 publicly disclosed cyber incidents involving U.S. public schools. The best way to respond is to collaborate in real-time with peers in a trusted sharing community. Attend the informational webinar on August 29 at 1pm ET. Register here

**Final Call for Speakers**
Last call! Join GRF as a presenter at the 6th Annual Summit on Security & Third-Party Risk, October 11-12, 2023 at the AT&T Conference Center in Austin, Texas. Submit to speak and share how your team has overcome security challenges, mitigated risk, or enhanced operational continuity practices.

Practitioner-presenters will cover topics like advanced monitoring, cloud due diligence, mitigating geopolitical impacts to supply chains, building vs. maturing a TPRM program, and maximizing the use of threat intelligence. Also included will be sessions on security use and management of AI, and its impact on third-party risk. Learn more

**Community Contacts**
OT-ISAC (John Lee)
LS-ISAO (Raquel Santiago)
EASE (Tim Chase)
ProSIX (Mark Orsi)
K12 SIX (Doug Levin)
BRC (Chris Denning)
Manufacturing ISAC (Tim Chase)
ONG-ISAC (Roderick Austin)
Newsletter contact (Pat McGlone)