
IN THIS ISSUE: OT-ISAC Has BEEN Busy!

OT-ISAC

In collaboration with Tenable, OT-ISAC is hosting a Capture the Flag event. Members will experience the thrill of solving real-world security challenges in a safe and simulated environment. They will compete with other players to identify compromised assets and vulnerabilities and identify ways to mitigate a future attack. With each challenge completed, members will gain a deeper understanding of how to defend against cyber threats. Ready to take on the ultimate cybersecurity challenge? Join the event on June 6, 2023 in Singapore. Contact aeserjose@grf.org for more info.

OT-ISAC continues to strengthen support to community members in the Philippines. The community delivered OT Security Awareness Training in April 2023. The course provided attendees with insight into the latest OT threats, industry standards and best practices, and recommendations to reduce cyber risk in OT environments.



OT-ISAC's John Lee joined Industrial Cyber to discuss inside threats in OT cybersecurity. "Red flags or threat indicators such as peculiar behaviour, unauthorized entry or attempts to systems, data theft/exfiltration..." [Read the full interview](#)

OT-ISAC partnered with Deloitte to produce the white paper "Bridging the Gaps in OT Cybersecurity Programs." Below are some key findings and recommendations.

- Risk assessment is crucial. Be sure to identify vulnerabilities and potential threats to OT systems. This includes identifying critical assets, analyzing potential risks and impacts, and developing mitigation strategies. Management must demonstrate a commitment to cybersecurity and prioritize it as a critical business function.
- Training and awareness are essential. Be sure to educate employees and stakeholders about OT cybersecurity risks and best practices. Cybersecurity is everyone's responsibility, and a culture of security awareness is essential for effective OT cybersecurity programs. Ensure that employees, including management, are trained and aware of their roles and responsibilities in maintaining OT cybersecurity.
- Collaboration is key. Collaboration enables the sharing of knowledge, expertise, and resources, which can help organizations identify and mitigate vulnerabilities and threats more effectively. There should be collaboration between IT and OT teams in order to develop effective OT cybersecurity programs. They have different priorities and responsibilities but working together is essential to ensure reliability of OT systems.

[Access the whitepaper](#)

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

LS-ISAO

Members, join LS-ISAO for a workshop in Chicago on July 13th at the Dentons law offices. The full agenda will be released soon. The community will also be hosting a Table Top Exercise with CISA in July. Contact rsantiago@grf.org for more information.

K12 SIX

The K12 SIX Essential Cybersecurity Protections Series – developed by K-12 IT practitioners, for K-12 IT practitioners and aligned to cybersecurity risk management best practices—establishes actionable baseline cybersecurity standards for U.S. school districts and provides guidance and tools to support their implementation. As highlighted in a recent webinar, [“Kickstarting Your K-12 Cybersecurity Program: Where and How to Start,”](#) the K12 SIX school district self-assessment was recently updated to incorporate planning tools to assist school systems in closing the gaps in identified weaknesses. As part of the process of making 2023-2024 school year updates to the series, K12 SIX is also pleased to announce an open call for feedback and input. For more information and to contribute your thoughts to this important initiative, check out the [K12 SIX Essentials Series](#).

Business Resilience Council

The Business Resilience Council (BRC) is a nonprofit, multi-sector community that allows members to collaborate on significant threats, incidents, regulations, and technologies that impact business operations. The BRC provides businesses with all source, multi-sector information sharing, an award-winning framework for operational resilience, a connection for third-party and vendor security, and an exercise program for testing and guidance on plans.

Business Resilience Council cont...

The BRC produces multiple intelligence products each day and hosts several community and working group meetings each month. Members of each of GRF's affiliated communities receive complimentary access to the BRC, and organizations which are not members of a GRF community may also [join](#). Some upcoming activities:

- The BRC's next webinar will be at 2:00 pm ET on June 7 with Brian Urbancic, Chief Meteorologist at Early Alert. Brian will present a 2023 Atlantic hurricane season forecast. The complimentary webinar will also cover recent topics which impact business resilience in physical and cybersecurity, and geopolitics. [Register here](#)
- On June 15, the BRC will host an exercise testing supply chain resilience and security against potential disruptions caused by a conflict between China and Taiwan. [Learn more here](#)



Call for Speakers

The 2023 Summit on Security & Third-Party Risk will be held October 11-12 in Austin, Texas. Submit your presentation topic today! [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](#))