TLP:CLEAR

MTS-ISAC

2023 Annual Report

Maritime Transportation System

Information Sharing & Analysis Center

Helping Build the Maritime Cybersecurity Community



TLP:CLEAR

About the MTS-ISAC

The Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC) is a nonprofit organization formed in February 2020 by a group of public and private sector maritime critical infrastructure stakeholders to promote cybersecurity information sharing throughout the MTS community. It is focused on providing **actionable, relevant, and timely cyber threat intelligence** shared from trusted MTS private and public sector partners – with further analysis and enrichment by the MTS-ISAC – to help provide the early warning needed for maritime stakeholders to defend themselves from cyber-attacks.

The MTS-ISAC's Nonprofit Mission

Promote and facilitate maritime cybersecurity information sharing, awareness, training, and collaboration efforts between private and public sector stakeholders to effectively improve cyber risk management across the MTS community through improved identification, protection, detection, response, and recovery efforts and to serve as the maritime sector's information exchange center of excellence.

MTS-ISAC Stakeholder Operations at a Glance

Across	In over	Part of	Includes
6	160	$10 trillion	**Shipping**
Continents	**Countries**	**Global Supply Chain, Transportation, and Logistics Industry**	**Energy**
			Cruise
			Logistics
			Rail
			Air Freight
			Offshore

Letter from the MTS-ISAC

We sincerely appreciate all the support we received from our public and private sector stakeholders during 2023! Progress continues to be made across our community as stakeholder programs continue to mature and community sharing of efforts continues. While our primary focus is on daily, tactical threat information sharing, operational and strategic efforts to share lessons learned and best practices also continue. The *actions* that our stakeholders take to make the sector more cyber resilient every day of the year is what counts, more so than any of the words here could possibly do. Our stakeholders' drive and focus on supporting this community mission continues to make a positive difference and we salute them for their efforts.

In cybersecurity, every year always seems to be more challenging than the previous year. Threat activity continues to expand, and more resources seem to be devoted toward policing victims of cyber-attacks as opposed to countering threat actors and sharing timely, actionable information. This trend continued in 2023, providing stakeholders with additional challenges requiring them to focus additional resources on compliance rather than risk management activities. It appears this tendency will continue in 2024, which means the sharing of threat information between stakeholders will be more important than ever to allow organizations to benefit from early warning and threat information sharing resource efficiencies.

This annual report provides a high-level review of our 2023 efforts. While there are various viewpoints on how cybersecurity challenges should best be addressed, there seems to be consensus that when stakeholders can pool resources and collaborate, progress occurs more quickly, efficiently, and effectively. We were excited to see our stakeholders' continued collaboration on threat information sharing and best practices across the year, culminating in an excellent Maritime Cybersecurity Summit in November. Throughout the year we saw the MTS-ISAC community dwarf other entities in terms of the amount of actionable, relevant, and timely cyber threat information that was shared.

More challenges await all of us in 2024. After four years of operations, our community continues to grow and understands very well that they are more resilient when they work together. We are grateful for the continued interest in the MTS-ISAC and the support from our stakeholders!

A special thank you to our Board of Directors, stakeholders, CIP IX, and interns! Private industry and local government stakeholders are frequently the entities out front leading the way in actionable threat information sharing. We appreciate everything you do to help make the sector more cyber resilient!

Stay safe *and* secure,

Scott Dickerson	Christy Coffey	John Felker	Analytics Team
Executive Director	VP, Operations	Senior Advisor	Security Operations Center

Please contact us at:

Website: https://www.mtsisac.org/contact/
LinkedIn: https://www.linkedin.com/company/mts-isac/

Contents

Our Stakeholders are Leading the Way

During 2023, our stakeholders continued their efforts in leading the international maritime sector in timely, actionable, and relevant cyber threat information sharing efforts. Industry leaders in shipping, terminal operations, cruise, energy, logistics, and offshore together with port authorities actively shared anonymized threat information with each other through the MTS-ISAC. Just one of our stakeholder shares can contain a dozen or more emails in a zip file, a log with thousands of IP addresses, or a list of hundreds of indicators associated with ransomware, but each is counted as a single share. Our community-minded stakeholders contributed **nearly 2,300** of these shares over the course of the year to help make the sector more aware and resilient to cyber-attacks from a variety of threat actors. Our community understands the interconnected and interdependent nature of their operations, and whether it could impact partners or competitors, the system of systems would be negatively impacted if critical threat information was not shared. As a result, our stakeholders are actively engaged with the broader community.

"Only when we come together as a community and share information with each other, can we start to see the blind spots that may exist. The MTS-ISAC has been instrumental in providing valuable insights on ongoing cybersecurity threats in the maritime industry."

Paul Lim, IT Security Section Head,
Ocean Network Express Pte. Ltd.

In addition to sharing actionable threat information, stakeholders actively participated in a variety of analyst calls, webinars, working groups, and meetings throughout the year. These events allow the MTS-ISAC to provide greater details on trends and threat actor campaign activity, including details related to identified campaigns across dozens of threat actor groups, malware (including ransomware) families actively being used, exploited vulnerabilities, and cyber defense best practice recommendations. These forums allowed international stakeholders to have improved situational awareness of what is happening across the maritime industry and beyond any singular geographic region.

The MTS-ISAC and its stakeholders also continue to work with a variety of international organizations, including the International Maritime Organization (IMO), International Association of Classification Societies (IACS), International Association of Ports and Harbors (IAPH), Baltic and International Maritime Council (BIMCO), and national government agencies, among others, to inform their cybersecurity guidelines and recommendations, proposed regulatory changes and implementation plans, and others on the realities, challenges, and practical aspects of international cybersecurity program efforts. This strategic guidance plays an important role as well in addressing common challenges related to the multifaceted aspects and implications of new rules and requirements being asked of international industry stakeholders when it comes to cybersecurity, especially around incident handling and reporting.

MTS-ISAC's Delivery to Stakeholders in 2023

Provided	Contributed		Produced	
42	5	2,284	69	1,330
Collaboration Opportunities	**Best Practices & Templates**	**Intelligence Shares**	**Cybersecurity Advisories**	**MTS Indicator Bulletins**

2023 Attacks Targeting Maritime Transportation System Stakeholders

We believe it is well understood that the number of cyber-attacks continues to increase year over year and impacts all industry segments. This trend is expected to remain as digital divides continue to shrink and more assets, applications, and networks become integrated across the MTS around the world. In 2023, this was highlighted by multiple nation-states, advanced persistent threat (APT) actors targeting the sector in espionage and preparatory campaigns. Criminal threat actors also targeted the sector with multiple ransomware campaigns as well. In general, MTS stakeholders around the world are experiencing increased cyber threats and risks to their operations, which inevitably threatens global supply chains and economies around the world.

Among the contributing factors to increased MTS cyber risks are:

- Ongoing geopolitical tensions due to wars and conflicts, with multiple countries aiding one side or the other either directly or by expressing their support.
- Due to a variety of challenges in countering and punishing nation-states and criminals for cyber-attacks, cyber-attacks remain a relatively low-risk endeavor for many threat actors. As such, there are few punitive measures severe and frequent enough in multiple geographic areas to dissuade against conducting attacks in cyberspace. **Instead of countries attempting to hold the dozens of threat actor groups launching these attacks accountable, some countries are choosing to police the victims of cyber-attacks and blaming them.** In many ways this situation parallels how victims of assault have often been treated by legal systems for decades.
- Following the economic measures put in place around the world due to the COVID-19 pandemic, inflation and recessionary market pressures are impacting economies around the world. An untold number of workers may be underemployed or unemployed and could turn to cybercrime as a means to survive in struggling economies.
- The maritime industry continues to modernize, and the number of third-party integrations continues to increase. This provides a target rich environment across an industry where organizations may lag behind other industries in terms of cybersecurity maturity and investments.

The below graphic underscores just some of the active campaigns seen in 2023.

Threat Activity Highlights by Quarter			
Q1	**Q2**	**Q3**	**Q4**
Seaborgium and Mustang Panda APT activity; AlphV, LockBit 3.0, Play, and Royal ransomware.	**Volt Typhoon, Seaborgium, TortoiseShell APT activity; Cl0p ransomware; Snake malware espionage.**	**New malware variants, increased password spraying and aggressive zero-day vulnerability probes.**	**Overall phishing decreased, but with an increase in credential harvesting payloads from BEC senders.**

Advanced Persistent Threats

The MTS-ISAC correlated many 2023 stakeholders shares with various APT attacks conducted by the governments of China, Democratic People's Republic of Korea, Iran, and Russia as reported by security researchers and a variety of national agencies, including the following, among others:

- Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (CCCS)
- New Zealand National Cyber Security Centre (NCSC-NZ)

- U.K. National Cyber Security Centre (NCSC-UK)
- U.S. Cybersecurity and Infrastructure Security Agency (CISA)
- U.S. Federal Bureau of Investigation (FBI)

As a result of information sharing from stakeholders, the MTS-ISAC was able to **correlate information with over 18 APT actors** and report specific APT actor attack information to our stakeholder community. The MTS-ISAC also contributed 9 incidents that occurred between November 1, 2022, and October 31, 2023 to Verizon for inclusion in their **2024 Data Breach Investigations Report** (DBIR).

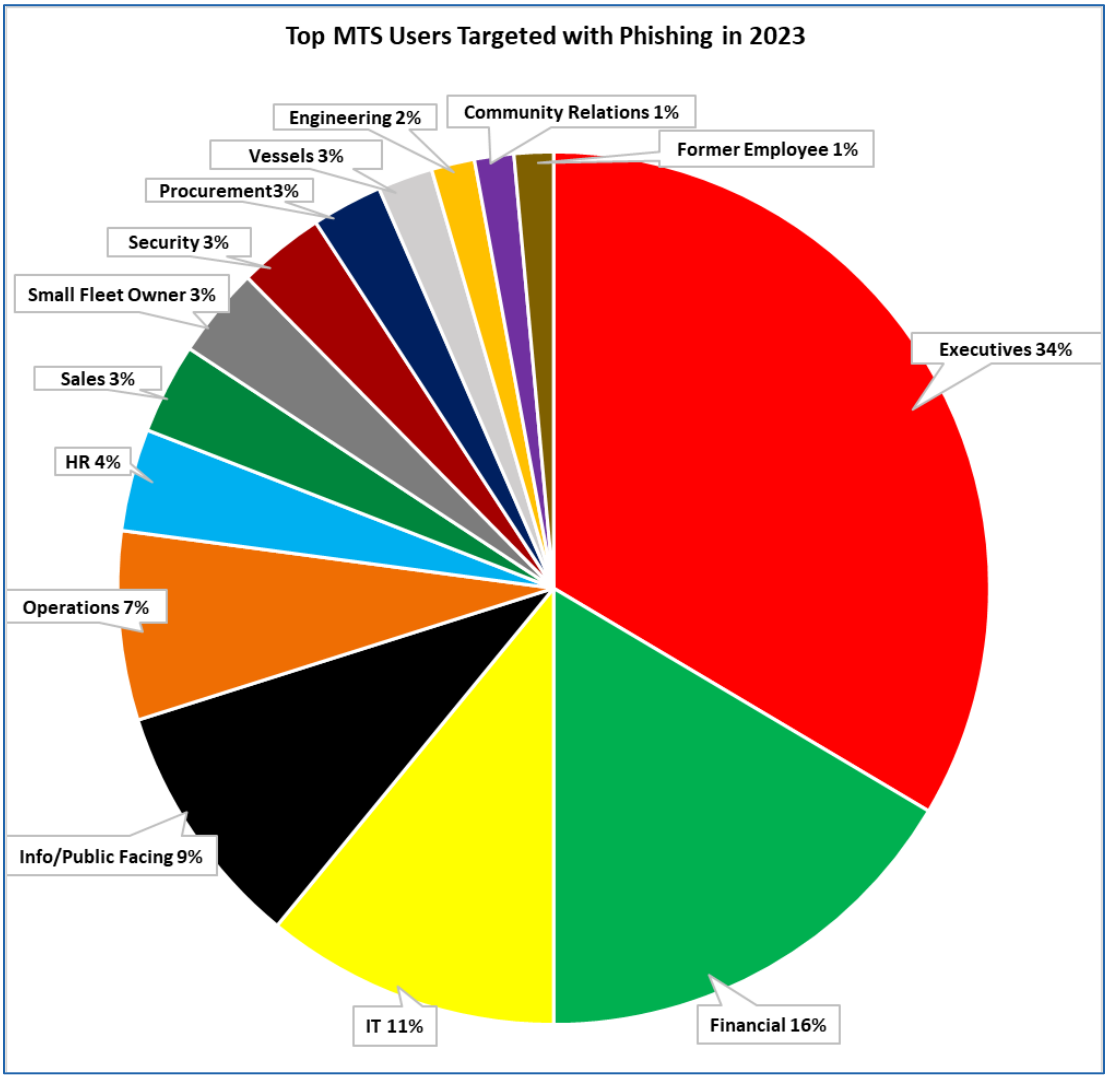
"While it is nearly impossible for companies to protect themselves against all cyber-attacks, having situational awareness of threat activity helps businesses take prudent measures. Matson is supportive of the MTS-ISAC community. We believe the anonymized sharing of cyber threat information among stakeholders is a difference maker in allowing companies to respond quicker and limit the impacts."

Sean Walsh
Senior Director, Information Security
Matson Navigation Company, Inc.

Phishing

Every week MTS stakeholders reported phishing attempts, some of which were unblocked by email security solutions, targeting both ship and shoreside personnel. The MTS-ISAC continues to see common trends of threat actors spoofing vessels, government organizations, executives, MTS organizations, and vendors as the email senders. In addition, legitimate operational procedures, vessel names, port state control, and other industry specific references are used as lures. Through analysis of the reported phishing attempts, the MTS-ISAC reported on a variety of tactics, techniques, and procedures (TTPs) related to credential harvesting, attempted intellectual property theft, financial fraud, and other campaigns. Stakeholders received updates on phishing trends through weekly reports, monthly analyst roundups, quarterly reports, and via threat advisories.

Throughout 2023, adversaries continued their use of cloud-hosted "free" services to deliver emails and/or malicious payloads, host redirect links, and the use of Google, Microsoft, Cloudflare, and other difficult to block infrastructure to host malicious downloads to counter security control efforts. Threat actors also used QR codes and "meddler-in-the-middle" to circumvent multi-factor authentication (MFA) controls or to steal web connection and session information to gain access. **Phishing training should remain an essential element of every cybersecurity awareness training program as the end user is too frequently the last line of defense to prevent security incidents.**



Smishing

Smishing (SMS phishing) attacks were reported by MTS-ISAC stakeholders throughout the year. MTS users frequently reported receiving smishes spoofing their executives on both their work and personal devices and were even sent to family members upon occasion. Many of these messages were void of malicious links and were social engineering in nature trying to solicit an initial response.

Malware

During 2023, the MTS-ISAC tracked over a dozen malware variants, including new malware variants that sometimes included maritime amongst the first industries targeted by threat actors. Among the common malware reported were: AgentTesla, Emotet, SnakeKeylogger, FormBook, LokiBot, Remcos RAT, Qakbot, LummaC2 Stealer, and Venom RAT. Based on analysis, these variants intended to steal information, create backdoors, install keyloggers, and in some cases included worm-like capabilities. Malware analysis of these emails became more intricate, making it difficult to identify where the payload originated, and sandbox evasion techniques were consistently implemented. MITRE ATT&CK matrix analysis identified behaviors such as persistence and privilege escalation at boot or start-up.

"We have been so happy to support the MTS-ISAC's trusted global sharing community for the past four years. At the Cyber-SHIP Lab Symposium at the IMO in November 2023, where the expansion of the sharing community clearly became a top priority agenda item, it was terrific to see the MTS-ISAC's leadership providing concrete, real-world examples of the daily, actionable, and relevant sharing taking place across its community. While others talk about the need to share, the MTS-ISAC continues to lead the way by actually doing it!"

Makiko Tani, Deputy Manager, Cyber Security Team, ClassNK

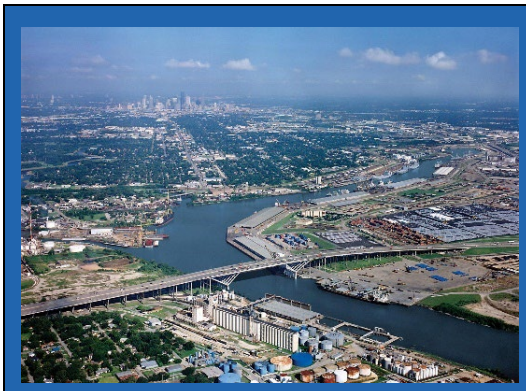
Ransomware

It was prevalent across the year and this nation-state sponsored and criminal activity undoubtedly will not show any signs of dissipating, hence the pervasiveness of so many ransomware-as-a-service (Raas) threat actors. Threat actors are constantly scanning networks searching for zero-day vulnerabilities, probing for misconfigured ports, and password spraying virtual private networks looking for single-factor authentication users which could provide an entry point for ransomware or other nefarious activity. The MTS-ISAC provided reporting across the year related to 8Base, Akira, AlphV, BianLian, BlackBasta, BlackByte, Cl0p, HiveLeaks, LockBit 3.0, Play, RansomHouse, Ragnar, Royal, and roughly a dozen others.

"When we partnered with the MTS-ISAC, our cruise line members instantly benefited from collaboration with other maritime stakeholders and visibility into cyber threat activity targeting the broader maritime sector."
Mr. Donald Brown
Senior Vice President, Maritime Policy
Cruise Lines International Association

Scanning for Vulnerabilities, Password Spraying, Denial of Service, and Probes

Aggressive brute-force attacks that targeted both active and common VPN user accounts and Azure PowerShell were reported to the MTS-ISAC. Password spraying was commonly reported, as were vulnerability probes and scanning. Stakeholders also reported IP addresses conducting aggressive Microsoft Active Directory probing, Exchange Server probes, Apache Log4j remote code execution, F5 BIG-IP authentication bypass, scanner enforcement violations, application server(s) protection violations, website vulnerability probes, C2 traffic, webserver enforcement violations, remote code execution vulnerability probes, FTP brute force login attempts, Heartbeat vulnerability probes, unauthorized access



"The Houston Ship Channel Security District and MTS-ISAC are working together to provide a secure information network that aids its stakeholders with cybersecurity and more. MTS-ISAC has kept our members informed and given them the tools they need to combat the threats that put all our industries at risk. This allows a platform for stakeholders to interact with each other and share their concerns in a safe and secure manner. We look forward to our continued collaboration."

Angela Gonzalez, Administrator, Houston Ship Channel Security District

attempts to Outlook Web Access, and WordPress probes. In some cases, logs showed that individual personnel and/or departments were targeted more frequently; however, stakeholders also reported former employees, common names, and non-existent users being targeted. On occasion, users without multi-factor authentication in place were successfully breached. These compromised accounts were used to send phishing emails and possibly resulted in user lists stolen by threat actors.

NoName057(16), Net Worker Alliance and KILLNET were active in distributed denial-of-service (DDoS) attacks conducted against MTS stakeholders. Most DDoS attacks were unable to penetrate networks and only modestly impacted website assets. In most cases, DDoS protection in-place was effective in mitigating the attacks.

Similar to previous years, logs showed malicious scanning traffic consistently coming from universities, academic institutions, and research organizations regularly targeting MTS networks. Aggressive scanning, likely searching for access to Internet of Things (IoT) devices, was also frequently reported.

Collaboration Across the Community

It was another year of improving partnerships across the sector, as more organizations joined the MTS-ISAC and contributed to the community's public and private sector collaboration. We were excited to welcome the **Maritime and Port Authority of Singapore (MPA)** to the MTS-ISAC community as a leader in many international maritime security efforts, and the **Cruise Line Industry Association** to further expand the involvement of cruise lines alongside other maritime operators. In addition, several private sector stakeholders joined our community and immediately started being actively engaged.

"We share suspicious cyber threat activity targeting our organization to the MTS-ISAC, and advocate for other stakeholders to do the same. Having anonymized visibility of threat activity targeting the maritime community helps us all better prioritize our efforts to make the sector more resilient. In addition, the MTS-ISAC provides valuable analysis of threats and offers several working groups that are awesome. We find the services that the ISAC brings to the maritime community to be invaluable."

Davin Garcia, IT Manager, Port of Stockton

The **US Coast Guard, US Transportation Command (USTRANSCOM), and Federal Emergency Management Agency (FEMA)** regularly participated in Open Calls with MTS-ISAC stakeholders to provide updates on various program efforts and answer industry questions. The US Coast Guard, USTRANSCOM, **Federal Bureau of Investigation**, **Transportation Security Administration**, and the **Canadian Centre for Cyber Security** also participated in the Maritime Cybersecurity Summit.

The MTS-ISAC's Critical Infrastructure Partners Information Exchange (CIP-IX) saw new members, including the **Global Maritime Cybersecurity Consortium (GMCC)**, **ABS Group**, and **Red Vector** join alongside **Cyware** and **Booz Allen Hamilton**. These CIP-IX partners provided subject matter expertise into MTS-ISAC and supported multiple Working Groups and webinars across the year.

"Booz Allen is honored to be a CIP-IX member and a contributing MTS-ISAC partner. We welcome the opportunity to share our technical expertise in Operational Technology, Resilience, Cyber Risk, and the emerging topics of Artificial Intelligence, Post-Quantum Cryptography, and Zero Trust. We love that the Working Groups and stakeholders promote the exchange of information that helps strengthen the maritime community."

Heath Stockton, Principal, Global Growth, Booz Allen Hamilton

Enhancements to the Information Sharing Platform

Our information sharing platform, Cyware, added new capabilities in 2023. Major releases added new features that enhanced our ability to track and enrich data for the community. By creating custom fields in Cyware that have query and reporting capabilities, the MTS-ISAC is able to more easily produce a weekly MTS attack trends dashboard with patterns of activity to elevate threat awareness. Automated bi-directional information sharing between MTS-ISAC partners continued to improve, and stakeholders integrated Cyware with a growing list of sensors, endpoint devices, and security information and event management (SIEM) technologies to automate consumption of MTS and partner indicators.

Stakeholder requests for information (RFI) continue to be a useful process. Shore and shipside stakeholders are able to submit anonymous requests to the trusted global community on targeted threat activity, policies, best practices, and guidance. Whether looking for strategies to better protect ships, secure cloud infrastructure, and understand vendors and service provider risk, or managing port tenant relationships to improve situational awareness related to breaches, the community regularly responded to these RFIs.

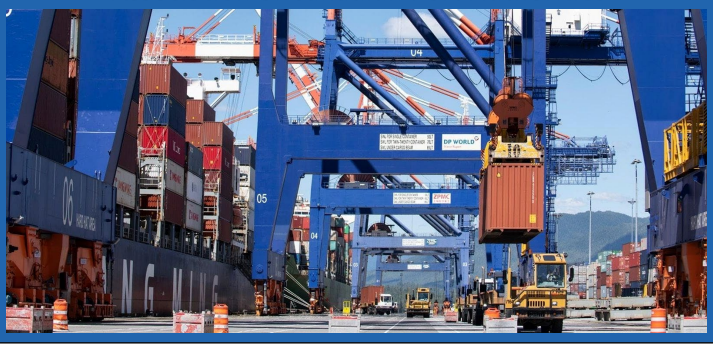
Setting an Example for Effective Industry Collaboration

The MTS-ISAC helped lead the community by publishing **18 TLP:GREEN advisories** related to sector-specific cyber threat information in 2023. In addition, the MTS-ISAC continued offering a **quarterly threat intelligence brief** for the MTS community at the TLP:GREEN level. These threat information products, created directly from cyber threat reporting shared with the MTS-ISAC by stakeholders, were available to both public and private sector organizations with an interest in maritime cybersecurity at no cost as part of supporting our nonprofit mission. In addition, the MTS-ISAC provided inputs to other industry groups' cybersecurity efforts, including IAPH, BIMCO, and IACS.

Events

Multiple webinars were held throughout the year. The MTS-ISAC co-hosted webinars with subject matter experts focused on topics of high interest, "Leveraging a Cyber Range to Minimize Cyber-Physical Systems Attacks" (with **Cloud Range Cyber**), "Securing Maritime OT: Lessons from a Heavyweight Attack" (with **Sygnia**), "Reduce Risk with Increased Trust – Insider Risk Management" (with **Red Vector**), "Connecting the Dots Between Threat Intel and Security Operations" (with **Cyware**), "Benchmarking Maritime Cybersecurity Against Other Industries" and "The Escalating Threat of Ransomware" (with **Booz Allen Hamilton**), and "Review of Commodity Malware and Phishing Challenges" (with **EclecticIQ**). Stakeholders were also invited to participate in a popular Capture The Flag event, hosted by **HackTheBox**.

"The MTS-ISAC is the leading source of expertise, knowledge, and networks for the port and marine industry on cybersecurity. Whether you are making long term policy, spending or planning decisions or need real-time and reliable information to make critical operational decisions, you will get the best information you need from this single source. And, the annual summit is an incredible event to hear best practices and connect with cutting edge thinkers, creators, and practitioners."
Debbie Murray, Sr. Director Policy and Regulatory Affairs, Association of Canadian Port Authorities



In addition, we were happy to support events hosted by other maritime organizations, including:

- Carnival's Maritime Cyber Safety Summit,
- The Global Maritime Cybersecurity Symposium hosted by Australian Department of Home Affairs,
- National Defense Transportation Association (NDTA) – USTRANSCOM Fall Meeting, and
- The Cyber-SHIP Lab / IMO Symposium.

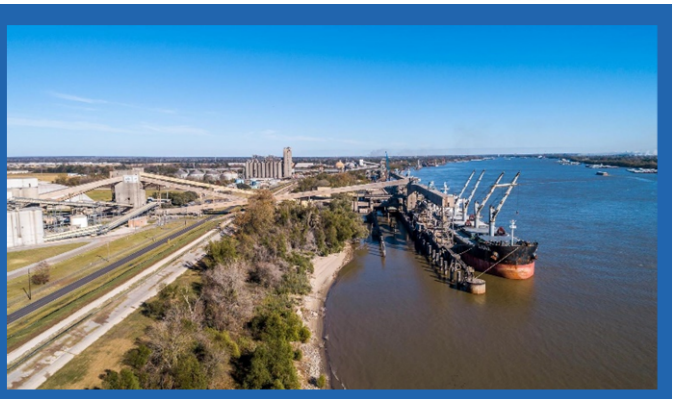
During the third quarter, the MTS-ISAC **developed and facilitated a tailored cyber tabletop exercise** (TTX) for a stakeholder. The TTX incorporated elements that truly showcased the complex elements of the international shipping industry and how a cyber incident can be a whole of organization challenge and required multiple departments outside of IT and Information Security to participate, including Operations, Legal, Physical Security, Government Relations, and others. Among the potential impacts discussed related to **real world APT activity targeting the maritime sector** were vessel operations, shoreside operations, corporate IT environments, and international cyber laws and reporting requirements. **Organizations greatly benefit from TTXs that incorporate these elements.**

Fifth Annual Maritime Cybersecurity Summit

From November 13-15, several of our stakeholders shared insights about their cybersecurity challenges and identified best practices during the **5th Annual Maritime Cybersecurity Summit** in Miami, Florida. We are extremely grateful for the speakers, sponsors, and attendees who supported and participated in the annual Summit. We were delighted that the Chief Information Security Officers (CISOs) from **Carnival,** Ms. Gatha Sadhir, and **Kaleris,** Mr. Luciano Ferrari, provided keynote addresses and for all of the domestic and

international speakers and attendees representing private and public sector stakeholders, academia, service providers, and associations! The Summit focused on delivering maritime cybersecurity practitioners with information and practical solutions to strengthen their core programs and reduce risk, and we were pleased that industry leaders contributed their unique perspectives, rich with a mix of vision and experience. We were also glad that our Critical Infrastructure Partners Information Exchange (CIP-IX) stakeholders were actively involved as well and supported a new inclusion to the Summit, a Practitioner Training Day, supported by the CIP-IX's GMCC. Subject matter experts from **Booz Allen, CISO LLC, Fullblown Security, Hudson Cyber, MAD Security,** and **Morse Alpha Associates** shared practical insights on how to effectively apply and integrate cybersecurity best practices into a variety of program areas.

Attendees leveraged their time together in Miami to gather strategies from their peers on how to advance cybersecurity in their respective organizations, network with subject matter experts, and meet with sponsors providing industry services and technologies. Every year the Summit strives to pull together a program which covers as much cybersecurity ground as possible to share and evolve best practices and accelerate our stakeholders' abilities to improve cyber defenses and manage organizational risk. We greatly appreciate everyone's support of this event!



"Recently, I had the opportunity to attend the MTS-ISAC's Maritime Cybersecurity Summit, and it was truly enlightening. The event brought together professionals from various industries, each sharing their insights and experiences in combating cyber threats. From engaging keynote presentations to interactive workshops and panel discussions, the conference covered a wide range of topics, including emerging threats, best practices in incident response, and the importance of user awareness training. One aspect that stood out was the emphasis on collaboration and information sharing. It was inspiring to see how organizations are coming together to address common challenges and enhance their collective defense against cyber-attacks. The networking opportunities were invaluable, allowing me to connect with experts in the field and exchange ideas on innovative security solutions and strategies."

Milton Corney, IT Program Manager, Port of South Louisiana

Looking to the Horizon

Much of our future prognosis remains unchanged as the cybersecurity situation in the maritime industry remains largely unchanged with several of the commonly cited concerns remaining in place. Chief among them, as the maritime industry continues to modernize, the number of third-party hardware and software integrations to support supply chain information technology (IT), operational technology (OT) and Industrial Internet of Things (IIoT) business requirements is continuously increasing. These digitalization efforts increase the attack surface as they introduce new vulnerabilities, providing a target rich environment for attackers. However, there are still legacy systems that will remain in operation for the foreseeable future as well. Given the interdependent nature of the transportation sector, this can create instances where both secure and insecure processes and technologies need to be accommodated to maintain a functioning supply chain. In addition, there are several other risk factors across the people, process, and technology aspects of the sector. As a result, multiple security organizations in the private and public sectors expect to see an increase in attacks targeting the supply chain, including campaigns targeting OT and IIoT assets. Sadly, there has been minimal progress made by governments to meaningfully counter the dozens of cyber threat actor groups, which subsequently requires tens of thousands of sector stakeholders to all defend against their attacks.

To improve resiliency, we need to hasten adoption of information sharing by industry stakeholders, including owners and operators, local authorities, suppliers, and key third parties. The sector needs greater collaboration as a whole, but especially between IT, OT, and IIoT equipment manufacturers, software developers, integrators, and owners/operators on cybersecurity efforts. The sector remains reliant on the experience of Masters, Chiefs, Terminal Engineers, etc. on a daily basis to ensure operations occur in a safe and secure manner, but those personnel rely on cybersecurity specialists and the aforementioned collaboration to make sure the systems they are operating are secure by design and implementation. Sharing cyber threat information across organizations, improving maritime cybersecurity training and exercises, and heightening situational awareness regarding not only the risks but the best practices to manage them, are all steps we can take as a community to improve the sector's resiliency.

"The MTS-ISAC is recognized as the leading cybersecurity information sharing organization in the maritime community. As we move into a complex and unknown future where cyber threats are rapidly increasing and often outpacing defensive resources, organizations can no longer risk combating cyber threats in a vacuum. The MTS-ISAC has created and grown a world class community of Maritime stakeholders that allows for the rapid sharing and exchange of critical cyber threats and intelligence information. Wärtsilä is proud to be one of the newest members of the MTS-ISAC and our Global SOC has found the information available to be critical in helping us protect and secure our global operations. As a global company we are uniquely positioned to observe and counter cyber threats from various threat actors around the world and look forward to supporting the MTS-ISAC as a stakeholder as we move together into the future."

Stephen Mills, Global Director of Navy Cybersecurity, Wärtsilä

To date, most national government agencies have been slower in their actions to support timely, actionable cyber threat information sharing than some of the critical infrastructure stakeholders they regulate or provide oversight for. This is continuing to exacerbate cyber risks across the sector. As many leaders know, sometimes it is important to be a good follower. Supply chain stakeholders may benefit more if government agencies were to offer support of industry efforts that are working effectively, rather than attempting to lead. As government agencies continue to "talk about" information sharing or "trying to understand" what needs to be done from an information sharing perspective, it slows the adoption of effective solutions. There is no panacea in cybersecurity, but there are measures proven to be effective. The MTS needs more national level leaders across the sector to be proactive in their support of the successful information sharing efforts taking place across the public and private entities that are ultimately responsible for daily supply chain operations. It will take the maritime cybersecurity community acting together to remain resilient in the face of ongoing cyber-attacks, and we're extremely proud of the efforts our stakeholders are taking to proactively move things forward.

Helping Build the Maritime Cybersecurity Community