TLP:WHITE

# MTS-ISAC

# 2021 Annual Report

## Maritime Transportation System

## Information Sharing & Analysis Center

*Helping Build the Maritime Cybersecurity Community*



TLP:WHITE

## Letter from the MTS-ISAC

At the end of 2020, many in the community felt we ended the year with a rare, but broadly impacting, type of campaign. There was no way we would see multiple campaigns in 2021 that would be like that, right? Well, early in 2021 we quickly learned that it was going to be another year not to be reckoned with!

In 2021, we completed our first full calendar year of operations. Our second Annual Report highlights the incredible progress our community made last year, including key milestones and results achieved. We believe it is an amazing testament to the dedication and devotion to duty of everyone involved in supporting our mission and this community. The effectiveness of the MTS-ISAC is dependent upon the active engagement of our stakeholders, and thankfully we have a very engaged group of them!

From tackling significant vulnerabilities in multiple products that are widely implemented to identifying and staving off advanced persistent threat (APT) actors, stakeholders worked relentlessly to keep maritime operations moving this past year. Several leveraged Information Exchanges to allow stakeholders to work more closely together and create a common baseline understanding of the cyber threats they are facing. At the end of the day, community approaches are adding value across the sector.

Much work remains. The good news is that there are true leaders among our critical infrastructure stakeholders, those local government agencies and businesses that own, operate and are responsible for securing critical infrastructure, which are leading the way! We will continue to engage national agencies on the need to share *timely, actionable and relevant information* with stakeholders and to support collaboration efforts. We believe the MTS will be more resilient when we achieve true public-private information sharing and collaboration across the sector.

From all of us at the MTS-ISAC, we appreciate your support! Thank you!!

Stay safe *and* secure,

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

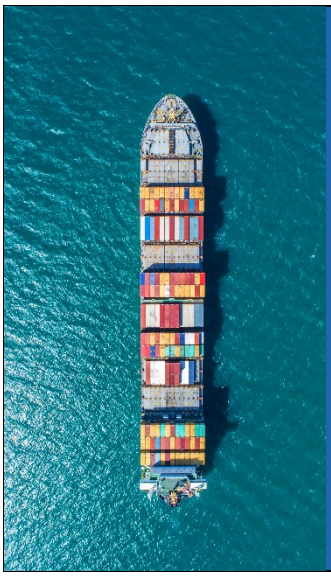
**Contact Information**

Please contact us at:

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

## Contents





**"Supply chain visibility relies on all stakeholders being able to exchange data. This means systems must be interlinked and interoperable. As we drive adoption of DCSA digital standards in the industry to enable interoperability, it is critical that cybersecurity is built into these standards and becomes a core competency of every organization to ensure overall protection of the supply chain. By being part of the MTS-ISAC community, DCSA and its members have the support and information to ensure a strong defence against cyber threats."**

**Henning Schleyerbach, Chief Operating Officer,**
**Digital Container Shipping Association (DCSA)**

## Growth from a Solid Foundation of Community, Leadership and Trust

The MTS-ISAC's community of maritime transportation system (MTS) stakeholders rose to address every known cybersecurity challenge presented in 2021. Whether it was MTS critical infrastructure stakeholders fending off attacks from advanced persistent threat (APT) actors, responding to aggressive scanning activity related to a wide-range of vulnerability disclosures, tracking and trending cybersecurity campaigns that dogged our industry month-after-month, or just getting through the daily grind, the realization and appreciation that we are stronger together shined. Rapid, successful incident response was a difference maker against determined adversaries. Meanwhile, proactive intelligence shares provided early situational awareness for other stakeholders to help protect our collective MTS community.

Across 2021, collaboration took many forms. The MTS-ISAC released 89 cybersecurity advisories sourced from stakeholder shares. We held analyst calls to collaborate on the latest threat trends, webinars on high interest topics, and working group and open calls to promote stakeholder awareness. The launch of our **Cyware** information sharing platform enabled rapid dissemination of intelligence, correlation to historic shares, and automated consumption of threat indicators. Exercises provided answers to "what if" scenarios so that cybersecurity controls related to people, processes, and technology could be fine-tuned to improve steady state operations while unexpected and unfavorable conditions could be equally accommodated. Partnerships with **The Norwegian Maritime Cyber Resilience Center (NORMA Cyber)** and **France Maritime Cyber** expanded our ecosystem and provided additional context for threat activity targeting our stakeholders.

However, our crowning achievement in 2021 was working with the **Port Authority of New York and New Jersey**, **Port Houston**, **Jacksonville Port Authority**, **Port of New Orleans**, **Port of Vancouver USA**, and the **Digital Container Shipping Association** to operationalize their respective **Information Exchange (IX)**. These IXs support security, safety, and continuity of business operations by bringing together distinct communities to better understand cyber risks and coordinate cybersecurity efforts and programs while connecting with the MTS-ISAC's global community of trusted maritime critical infrastructure stakeholders.

**"In its first year of operation, the Port of New York and New Jersey's Security Information Exchange has been instrumental in ensuring key port stakeholders have access to critical, timely, and actionable intelligence to protect their systems. The MTS-ISAC has been the cornerstone of this effort and continues to be an outstanding partner."**

**Michael Edgerton, Port Security Manager, Port Authority of New York & New Jersey**

In hindsight, we had a unique vantage point in 2021 because of the volume and consistency of sharing from MTS stakeholders. This annual report will take you through our collective journey, but here is an operational snapshot of the MTS-ISAC's second year:

| Launched | Responded to | Received | Published | Generated |
|---|---|---|---|---|
| 8 | 60 | 1,452 | 89 | 753 |
| **Information Exchanges** | **Requests for Information** | **MTS Intelligence Shares** | **Cybersecurity Advisories** | **Indicator Bulletins** |

## 2021 Attacks Target Maritime Transportation System Stakeholders

Based upon the reporting we received in 2021, MTS critical infrastructure stakeholders saw a marked increase in cyber-attacks from the previous year. Vulnerability disclosures and incidents experienced by MTS vendors, service, and infrastructure providers added to the chaos and unfortunately became an all-too-common experience. In addition, APT actor interests ranging from espionage and intellectual property theft to monetary gain plagued the year. **Even though stakeholders did experience zero-day exploits, ransomware, and data exfiltration attacks, having detection systems, procedures, back-ups, and trained users in-place allowed cyber defenders to quickly identify these threats and respond quickly and effectively. Great job to our stakeholders in maintaining their resiliency!**

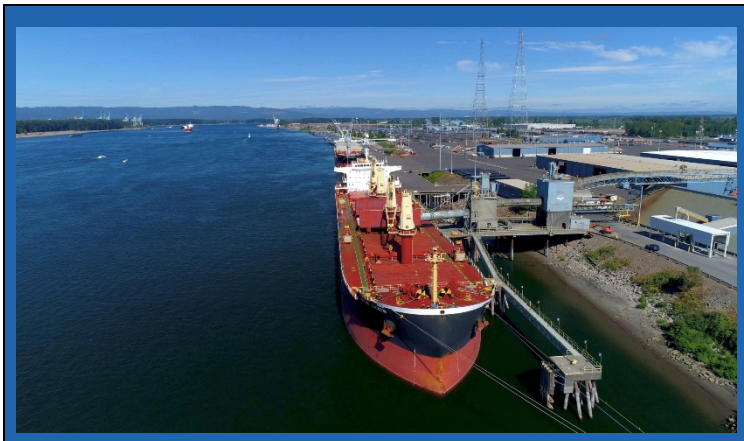
Joint efforts between Federal offices and technology providers resulted in multiple threat actor groups responsible for targeting MTS critical infrastructure stakeholders to be impacted in 2021. However, any relief in diminished threat activity was only temporary in nature. While the impetus for specific attacks remains unknown to the MTS-ISAC, there are multiple factors that likely contributed to an environment that led to the increase in attacks, including:

- Geopolitical tensions remained high between some nation-state cyber threat actors and the multiple countries where their victims were located;
- The global economy has been impacted by the COVID-19 pandemic. An untold number of workers worldwide are underemployed or unemployed and may turn to criminal activities to survive in a struggling economy;
- Due to a variety of legal challenges, cyber-attacks remain a relatively low-risk endeavor for many threat actors, who may act on behalf of government parties and/or receive protection from their local law enforcement;
- Insecure public-facing infrastructure, phishing and the prevalence of remote worker access has proven to be successful and inexpensive attack vectors; and
- The maritime industry continues to modernize, and the number of third-party integrations continues to increase, providing a target rich environment in an industry where organizations historically have not adequately resourced their IT and security teams even during peak economic times, and in which they may have further cut cybersecurity efforts because of the pandemic.

Which cyber risk items trended high for our stakeholders across 2021? Were there unique cybersecurity threats targeting maritime?

Here are some of our findings.

**"The MTS-ISAC allows me to collaborate with my colleagues in the maritime industry in an effective, secured environment of trusted expert partners. This collaboration is invaluable in assessing how my organization's cyber posture compares to others in the same industry and how we help each other make our networks that much more secure."**
**Davin Garcia,**
**Information Technology Manager,**
**Port of Stockton**



**"The Lower Columbia River Maritime Information Exchange (LCR-MIX) will improve the resiliency of this important waterway. So often, we see cyber threats that have the potential of impacting multiple LCR-MIX stakeholders. Now we can all have the same level of situational awareness."**

**Chris Carter, Information Security Analyst, Port of Vancouver USA**

**Phishing**

Phishing emails, both blocked and unblocked by technology solutions, were reported by MTS stakeholders nearly every day. Having visibility to so much threat activity provided MTS-ISAC analysts a view of the common tactics, techniques, and procedures used. It also led to a better understanding of threat actor motives, such as MTS intellectual property and credential theft.

Business email compromise of 3rd parties working with MTS critical infrastructure stakeholders continued to be problematic. Threat actors spoofed vessels, executives, MTS organizations, and vendors as the email senders and augmented their phishing attacks with fake websites and LinkedIn profiles. Of course, there were trojans, malware, and plenty of ransomware discovered from the reported attacks as well.

**In mid-May the MTS-ISAC received an unblocked email from a maritime stakeholder who supports energy as one of their lines of business. During analysis, an executable was dropped and data exfiltration was observed. This activity correlated with reports of an Advanced Persistent Threat group. Three weeks later a second maritime energy stakeholder reported an unblocked email that dropped the same executable. Having both of these shares provided the MTS-ISAC an opportunity to alert the community, and monitor for additional activity, trends and patterns.**

**Ransomware**

Across 2021, MTS-ISAC stakeholders reported phishing emails containing ransomware strains of CryptoLocker, Sodinokibi, Avaddon, GandCrab, Satana, Ryuk, Nibiru, CL0P, Virlok, and Conti. **The number of reported phishing emails with ransomware payloads increased by 300% from the first quarter to the third**. While email defense products and services mostly proved effective, adversaries continued to find ways to bypass them.

Unpatched systems also contributed to MTS ransomware incidents in 2021. It should be noted that an increase in malicious activity targeting MTS stakeholder infrastructure was observed on and around the same time as other successful critical infrastructure attacks, such as the Colonial Pipeline ransomware incident. Also, while successful ransomware attacks against vendors and suppliers did not negatively impact MTS business operations, they grabbed headlines in 2021.

**Advanced Persistent Threats**

In 2021, APT actors exploited zero-day vulnerabilities and conducted phishing email attacks to target MTS stakeholders. Given the consistency and regularity of stakeholder shares, MTS-ISAC analysts were able to

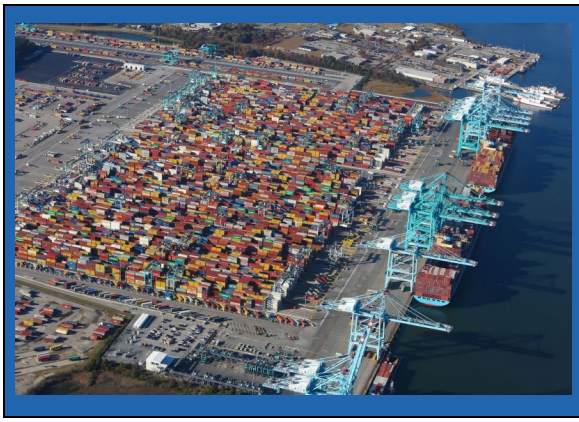
identify APT campaigns that targeted a single organization over a period of time. APT actors also targeted a group of maritime stakeholders with common business operations. In fact, eleven of the 89 cybersecurity advisories published by the MTS-ISAC in 2021 were related to APT activity. And, on occasion our shares correlated to APT-themed reports from US Federal agencies.

**Vulnerabilities, Scanning, Password Spraying, and Probes**

The SolarWinds Orion vulnerability which closed 2020 was quickly followed by the release of Exchange Server critical-out-of-band patches by Microsoft. The August discovery of a ManageEngine software zero-day vulnerability by Port Houston along with the Apache Software foundation release of multiple patches in December to address a critical vulnerability effecting it's Java-based logging utility Log4j, kept MTS critical infrastructure stakeholders scrambling to understand their risk exposure throughout the year. These vulnerabilities, and countless others released across the year, provided adversaries with ample opportunities and led to aggressive and regular scanning of networks, including those in the MTS.

Microsoft 365 credential stuffing attacks reported by MTS stakeholders across the year varied in intensity, with a dramatic spike reported in November. In some cases, logs showed that individual personnel and/or departments were targeted more frequently, or in some cases, after specific incidents, like the Colonial Pipeline incident. Probes of WordPress, Exchange Server, Outlook Web Access (OWA), and other external facing infrastructure were also reported. During the fourth quarter, multiple stakeholders reported a brute-force attack that targeted both active and inactive (old) VPN accounts.

Also, much like 2020, logs showed malicious traffic consistently coming from universities, academic institutions, and research organizations regularly targeting MTS networks. In fact, 150 CIDRs associated with education/research organizations were identified in December after analyzing logs associated with scans and probes. Finally, aggressive scanning, likely searching for access to Internet of Things (IoT) devices, was also reported.



**"The MTS-ISAC's ability to research suspicious cyber activity and correlate new information with previously reported MTS stakeholder shares, adds tremendous value for our security team."**

**Randy Plotkin, Information Security Manager, Port of Virginia**

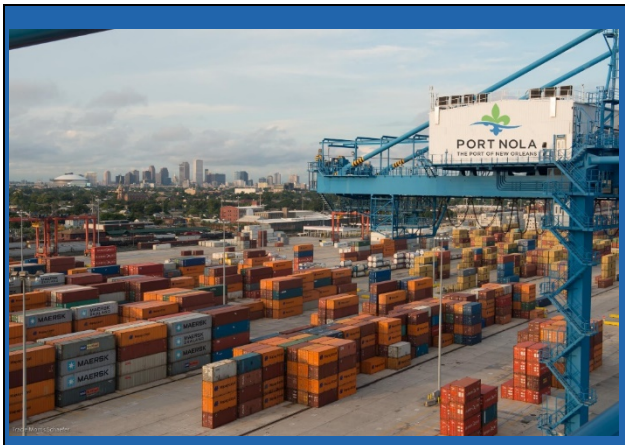
## Incident Response & Information Exchanges Deliver Operational Resilience

More than once in 2021, MTS stakeholders identified and stopped threat actors who breached the perimeter in 30 minutes or less. A combination of detection systems, procedures, and trained users enabled cyber defenders to quickly identify these threats. Then by reporting the threat activity to the MTS-ISAC, early situational awareness was provided to the community preventing future, similar attacks.

**Introducing an Information Sharing Platform to Operationalize Information Exchanges**

A community-of-communities approach was conceived of at the inception of the MTS-ISAC to counterbalance threat campaigns. Adversary campaigns, especially those that focus on breaching trusted third parties and then pivoting attacks within a trusted ecosystem, became the springboard for the

creation of regional or interest-specific communities within the MTS-ISAC umbrella. Regional communities not only provided a valuable source of actionable intelligence, but they helped speed the adoption of best practices and improved coordinated responsive through exercises.




**"As threat activity has accelerated and evolved, MTS-ISAC stakeholders rely on shared threat intelligence to improve awareness and threat response. Having the capability offered through the MTS-ISAC from Cyware gives us an easy, visible way to share and collaborate across the MTS-ISAC community quickly and effectively around critical threats to ports, infrastructure and shipping. This gives each MTS-ISAC stakeholder a new level of shared situational awareness."**
**David Cordell, CIO, Port of New Orleans**

Across 2021, seven IXs were operationalized, and **in the fourth quarter, IX community members contributed 71% of the total intelligence shares made to the MTS-ISAC!** To support these communities and provide a repository for historical shares, the MTS-ISAC introduced **Cyware**, a threat intelligence and information sharing platform. Not only did the implementation of Cyware improve stakeholder collaboration and increase situational awareness, but it also provided a STIX and TAXII interface for automated consumption of indicators into sensors, endpoint devices, and security information and event management (SIEM) technologies.

An eighth IX was formed in the fourth quarter to accommodate "**Critical Infrastructure Partners**" (CIP-IX) to provide vendors, suppliers, professional services providers, and others a unique opportunity to collaborate with our MTS community. We were excited that **Nozomi Networks** was the first organization to join the CIP-IX. Key objectives for the CIP-IX include increasing the MTS community's collective understanding of information related to emerging threats and patterns targeting MTS information technology (IT), operational technology (OT), and industrial internet of things (IIoT) systems and networks, reinforcing the adoption of cybersecurity and risk management best practices, and delivering support for incident response.

**"Cybersecurity is a critical part of supply chain security. We are thrilled to launch this important initiative, the Northeast Florida Maritime Information Exchange (NEFL-MIX), to protect our maritime community from cyber threats and ensure that our port-related businesses can continue to do the important work they do to keep cargo moving and people working throughout Northeast Florida."**
**Eric Green, CEO,**
**Jacksonville Port Authority (JAXPORT)**

## Enhancing Maritime Industry Cyber Resiliency Through Community

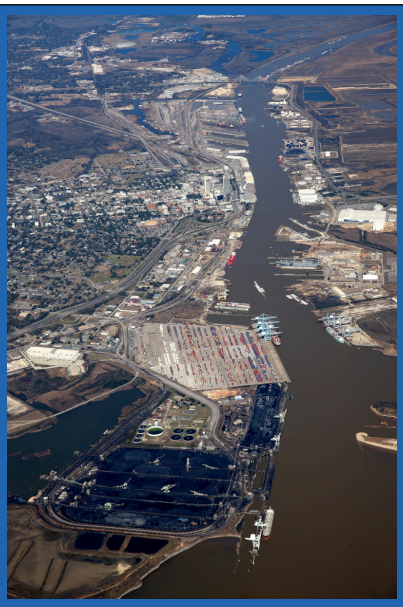
Across 2021, the MTS-ISAC contributed to the maritime cybersecurity community in meaningful ways. From advisories, exercises, and events, contributions to industry forums and new partnerships, to productive discussion with members of the U.S. Coast Guard and members of U.S. Congress, the MTS-ISAC worked for the benefit of the MTS community.

### Advisories

The MTS-ISAC published **89 cybersecurity advisories** across 2021, 35 of which were released at traffic light protocol GREEN instead of AMBER to broaden their circulation. Each advisory consisted of an executive summary of what happened, a section with threat activity indicators that a cybersecurity team could use to act, followed by best practice recommendations for consideration. **Content for advisories was created directly from cyber threat information shared to the MTS-ISAC by critical infrastructure stakeholders**. While some advisories documented trends observed over a short period of time, most were issued quickly to alert the MTS of active and potentially harmful activity.

As a result of excellent information sharing from stakeholders, the MTS-ISAC was able to contribute 12 incidents (that occurred between November 1, 2020, and October 31, 2021) to **Verizon** for inclusion in their **2022 Data Breach Investigations Report (DBIR)**. This is the MTS-ISAC's second year to contribute incident information for this prominent industry publication.

Also, several stakeholders issued requests for information (RFI) through the MTS-ISAC to better understand whether malicious cyber activity was targeting their specific organization, or the broader community. This approach to crowdsourcing targeting information was also leveraged to identify best practices and understand the effectiveness of different vendor products and services.



**"There are only so many hours in the day, and our priority has to be keeping staff, systems, and networks functioning. We find enormous value in working with our industry peers through the MTS-ISAC, to better understand where to prioritize and focus our attention."**

**Brett Valentz, IT & Network Infrastructure Manager, Alabama State Port Authority**

### Events

Across 2021, the MTS-ISAC provided several no cost learning opportunities for MTS stakeholders. Webinars, supported by subject matter experts and held on popular topics like "**Cybersecurity Guidelines for Ships**" with BIMCO, ClassNK, and Maersk, "**Data Breaches Two Takes, Two Motives – Financial versus Espionage**" with Verizon, "**Building a Security Operations Center**" with the Port of Virginia's Information Security Officer, Randy Plotkin, "**Developing and Implementing a Cybersecurity Roadmap**", "**Preparing for Ransomware**", "**How to Navigate Operational Technology (OT) Cybersecurity in Port Environments**", and "**Cloud Cybersecurity**" with Dirk Goehring, Director of Cybersecurity Information Technology for Crowley, and others. During webinars, attendees had the opportunity to interact both with the presenters and each other, which provided more opportunities for lively interaction during a year that limited many in-person opportunities to interact.

Additional stakeholder meet-ups included a quarterly M365 working group call, and monthly "Open Call" for stakeholders and then a second call with USCG Cyber personnel, which was introduced in the second half of the year. Also, a monthly "**Analyst Intel Round-up**" provided a venue to discuss threat activity trends observed in stakeholder shares, and impromptu briefings on critical vulnerabilities, like Apache Log4j and ManageEngine, were held.

**"An incident response plan was one of the first things that I put together when I got to the Port of Houston. We practice it, and it worked."**

**Chris Wolski, ISO, Port of Houston**

**During an MTS-ISAC briefing on the ManageEngine Zero-Day Cyber-Attack**

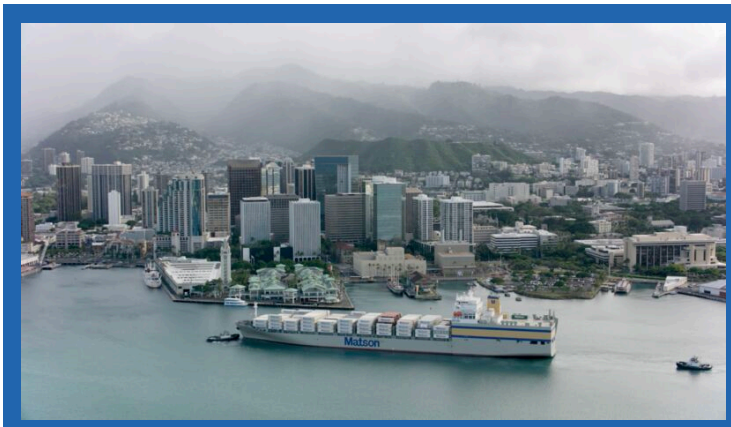
### Maritime Cybersecurity Summit

The MTS-ISAC joined as a "thought leader" sponsor for the 3rd annual Maritime Cybersecurity Summit (Nov 3-4) and participated on a panel with information sharing partners **The Norwegian Maritime Cyber Resilience Center (NORMA Cyber)** and **France Cyber Maritime**, also non-profits.

The 2021 Summit was well attended albeit virtually as COVID-19 travel restrictions limited MTS stakeholder travel. With subject matter experts participating from around the globe, this event provided a venue for candid conversation regarding the state of cybersecurity in the maritime industry and how we can work more effectively together to accelerate and improve resiliency. The MTS-ISAC is excited to bring the Maritime Cybersecurity Summit as an in-house event starting in 2022!

**Exercises**

For the second year, the MTS-ISAC led exercises for stakeholders. In the fourth quarter, the MTS-ISAC completed a **tabletop exercise** (TTX), which combined elements of **cyber, physical and insider threats**, for an MTS-ISAC stakeholder. We also participated in a second MTS-ISAC stakeholder's ransomware-themed TTX and contributed a cybersecurity inject for their exercise. Also, the MTS-ISAC continues to support TTXs held by various USCG Area Maritime Security Committees as an active participant and information sharing subject matter expert.




**"Exercises provide an opportunity to bring together various departments, along with external organizations, so that we can better understand how current security plans address an evolving threat landscape and how information should be shared during a crisis."**

**Sean Walsh, Senior Director, Information Security, Matson**

The MTS-ISAC supported other maritime cybersecurity initiatives across industry by:

- Supporting maritime cybersecurity calls hosted by numerous stakeholders and groups, including **Area Maritime Security Committees, International Association of Classification Societies, American Association of Port Authorities, FEMA's Port Security Grant Program,** and others.
- Briefing DHS' Cyber Information Sharing & Collaboration Program (CISCP) community at a Quarterly Technical Threat Exchange (QTTE) on "**Analysis of Reported 2021 Threat Activity**";
- Testifying before joint **Congressional committees** on cybersecurity challenges occurring in the transportation sector and participated in conversations with Congressional staff members thereafter to provide inputs on proposed legislation.

And, finally, understanding the need to develop the next generation of cyber warriors, the MTS-ISAC expanded its highly successful student Internship Program to include a second academic institution, Perdue University.

## Maturing Maritime Cybersecurity

So where do we go from here? The maritime sector continues to modernize at a rapid rate, but digital divides still exist around the world. While some port facilities, vessels, and offshore platforms continue to **integrate IT, OT, and IIoT systems and networks** to manage maritime operations more effectively, others are still highly reliant on manual control systems and processes. Given the interdependent nature of the transportation sector, this can create instances where both secure and insecure processes and technologies need to be accommodated. Elsewhere, the number of dependencies on third parties and integrators continues to rise. As a result, the MTS is more complex and integrated than ever before, which also increases the number of avenues an adversary can use to exploit a vulnerability to meet any number of objectives. In particular, we need IT, OT, and IIoT equipment manufacturers and software developers to be more transparent and willing to work with maritime owners and operators on cybersecurity efforts.

**"In a world of globally complex and connected business ecosystems, threat information sharing is no longer an area of competition and every ISAC of every industry should collaborate to support safe and resilient operations. As a classification society setting rules and standards for vessels engaged in international voyage, ClassNK welcomes and is committed to supporting MTS-ISAC initiatives to enhance a globally accessible platform for the entire maritime industry by expanding the community internationally and across the sector."**

**Makiko Tani, Deputy Manager, Cyber Security Team, Maritime Education and Training Certification Department, ClassNK**

Compounding the cybersecurity technical challenges that an organization may encounter, there are still several people and process issues that most organizations still need to address. The cybersecurity community needs to support operations personnel to make cybersecurity easier to understand and less of a scary, black box. We need personnel to comfortably understand the intent and importance of cybersecurity efforts. Doing so will provide a much-needed element of collaboration. **We rely on the experience of Masters, Chiefs, Terminal Engineers**, etc. on a daily basis to ensure operations occur in a safe manner. As new technologies are integrated, we need these personnel to **know how to use technologies both safely and securely to ensure operations remain "online"**. One place to look for guidance is the **International Association of Ports and Harbors' "Cybersecurity Guidelines for Ports and Port Facilities** (Version 1.0)", which was published in early September and shared with the International

Maritime Organization (IMO) for reference. While the guidelines cover a variety of cybersecurity disciples and efforts, an area of emphasis is to focus on the needed governance. Maritime organizations need to understand and act in a manner that recognizes **cybersecurity is an organizational challenge that requires the executive leadership team to take ownership and ac countability** for managing cyber risk. If the maritime sector understands and accepts this principle, then there is the possibility of maturing cybersecurity efforts across the sector more quickly, effectively, and efficiently.

## Looking to the Horizon

The good news is that there is **power in being involved with a community**. All of the challenges we face can leverage crowdsourcing when organizations are willing to exchange threat information, feedback on what solutions are working best for them, best practices they implemented, and collaborate on cybersecurity controls. Instead of multiple stakeholders tackling the exact same challenges, there is the opportunity to divide the work to gain efficiencies.

**"Supply chain attacks and a determined, capable, and evolving adversary make every day a battle. It's great to have the MTS-ISAC in our corner."**

**John Crochet, Director of IT, Port Fourchon**

Earlier we highlighted the work being done with the **Information Exchanges**. These are great examples of leadership, often by local governments, where a lead organization is ensuring that all stakeholders have access to the same threat information. This helps **close gaps in understanding and facilitates more meaningful collaboration** on strengthening common cybersecurity control areas.

The community needs to continue its work in shifting from a compliance mindset to a risk management one. While compliance will meet the requirements of an audit, it is largely inadequate when attempting to manage the cyber risks confronting an organization. Stopping at **a compliance threshold leaves organizations less resilient** as they will be more vulnerable to cascading impacts from cyber incidents.

While the future will always be uncertain, we look forward to exploring the opportunities it presents as we continue our work to help build the maritime cybersecurity community!

**"Crowley is pleased to be part of the MTS-ISAC cybersecurity information sharing community. Our participation alongside our industry partners plays an integral role in securing the data and systems critical to the maritime industry."**

**Dirk Goehring, Director of Cybersecurity Information Technology, Crowley**


**Special thanks to our board of directors, stakeholders, partners, collaborators, interns, and everyone who has taken an interest in supporting our mission!**


*Helping Build the Maritime Cybersecurity Community*