NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
January 2022 (Edition 2022-01)

This **electronic** publication is intended to inform port stakeholders about cyber security issues and provide information useful to safeguard seaport systems that may be vulnerable to cyber-attacks. The information contained herein is suitable for general release and members of the Northern California Area Maritime Security Committee are encouraged to pass it on to members of our maritime community. This newsletter will be e-mailed to members of the Northern California Area Maritime Security Committee and posted on the Coast Guard's HOMEPORT portal within the Sector San Francisco port area.

IF YOU SEE SOMETHING, SAY SOMETHING

To report a crime in progress, call 911 or your local police department. To report maritime related suspicious activities or breaches of security call the National Response Center (NRC) at 800-424-8802 or if a **cyber-attack** to the National Cybersecurity and Communications Integration Center (NCCIC) at 888-282-0870. After calling the NRC or NCCIC call the Captain of the Port, San Francisco, at 415-399-3530.

TABLE OF CONTENTS

ARTICLE SUMMARIES

- **Maritime Cybersecurity: A Rising Tide lifts all Boats** – discusses digital tools and the need for Information Technologists (IT) aboard ship.
- **Introduction: Cooperation on Maritime Cybersecurity** – discusses the Maritime Transportation System as a complex, interconnected environment, which relies information technologies; also has a link to the complete report.
- **Reminder for Critical Infrastructure to Stay Vigilant against Threats during Holidays and Weekends** – a joint CISA and FBI advisory with tips for protecting your information technology systems.

MAIN ARTICLES

Maritime Cybersecurity: A Rising Tide lifts all Boats, Mike Elgan, 06NOV2021

Ports and ships — the maritime industry — are vital points in the global supply chain for food, medicine, consumer goods, fuel and many other products. Most of the world's globally traded goods travel by sea. That's why maritime security is key for supply chain security. Meanwhile, maritime cybersecurity faces threats at multiple places, including ports, communications systems and ships themselves.

Potential cyber-attacks on maritime infrastructure are familiar types: phishing, malware, social engineering, brute force, denial of service, ransomware and others. What's different is the unique placement of the targets.

Ships Rely on Digital Tools

Ships often rely on digital tools to function, many of which are automated. Even ship compasses are digital and depend on a mix of gyroscopes and GPS. All these systems could be at risk for a digital attack. Dependence on GPS puts shipping at risk because attackers can spoof or jam GPS signals.

More than most industries, maritime infrastructure tends to be old and complicated, further hampering marine cybersecurity.

Is There an IT Worker on the Ship?

Another risk factor people don't talk about enough is the absence of IT people on ships. A ship is like a building packed with computer systems, servers and electronics. Yet, out at sea, the crew is on their own in managing these systems and dealing with breaches.

A digital attack could control or shut down a ship or drive it off-course, causing a crash. Some ships have dangerous cargo, such as explosive fuel, in large quantities.

Ports are also heavily dependent upon complex digital network logistics management systems. Some of these systems track every container on every ship. In the past, attackers have been able to delay, erase the knowledge of, redirect and steal actual cargo. They could abuse access to data on the location of cargo in a ransomware attack, or lock records.

The most likely risk is that digital attacks, through any number of possible attack types, delay shipping. That costs millions or billions of dollars to shipping companies, ports or shipping customers.

Maritime Cybersecurity Attacks Increasing

Attacks targeting maritime information systems are on the rise. In the first few months of the pandemic, attempted cyber-attacks rose by 400%. We can expect this trend to continue, with rising attacks on ships and ports.

Attackers targeted the Port of Houston this year in a suspected nation-state attack, an event that raised the urgency level of maritime security infrastructure. The port is 25 miles long and handles a quarter of a billion tons of cargo every year.

The attack involved a password management program that contained a formerly unknown vulnerability. The attackers exploited that to install malicious code that granted access to the networks, which they used to infiltrate log-in credentials needed to control network access. Luckily, "no operational data or systems were impacted," according to a statement issued by Port authorities.

How to Handle Maritime Cybersecurity Risks

The need to address maritime cybersecurity is urgent. Here are some general approaches for how to address it:

- **Pinpoint specific possible threats**. Understand what cyber criminals and nation-state actors might want from an attack. Pay special attention to the risk of ransomware. Consider attacks that could shut down the flow of goods, take ports offline and bring ships off course. Run red-team exercises and hire ethical hackers to help find likely attack points and methods.
- **Identify digital vulnerabilities**. Inventory all systems and figure out what are unpatched, un-patchable, legacy or problematic in any way from a cybersecurity perspective. Think through the implications of existing physical security, and figure out how unauthorized people could gain access to digital systems. Consider how rogue or disgruntled employees could threaten security.
- **Initiate a maritime cybersecurity action plan**. Address all vulnerabilities correctly, by patching or replacing problematic systems. Work with managers, leaders and stakeholders to develop these plans, then brief all concerned on how to use the plans in the event of an attack.
- **Install smart detection tools**. For example, network detection and response tools use artificial intelligence (AI) to find odd and potentially malicious behavior on maritime networks. Have your software working 24/7 to watch for possible emerging attacks.
- **Launch new crew and employee cybersecurity training programs**. Focus on phishing attacks, physical security and social engineering.
- **Establish contingency or continuity plans**. For each possible attack scenario, develop a detailed plan for running your business through it, and also what the recovery processes are.

A threat to maritime information systems is a threat to global trade. Therefore, supply chain cybersecurity is one of the world's most urgent business priorities.

Introduction: Cooperation on Maritime Cybersecurity, William Loomis, Virpratap Vikram Singh, Dr. Gary C. Kessler, Dr. Xavier Bellekens, 04OCT2021

INTRODUCTION

Oceans have long been the lifeblood of international trade and commerce. For more than five thousand years, humans have used rivers, lakes, and the seas to move goods from place to place quickly and efficiently. As civilizations continued to expand and better understand the strategic advantages of maritime trade, this usage accelerated. Initially logs bound together with rope, watercraft evolved into small, carved, wooden vessels. Before long, the first major trade routes began to surface—and the global maritime transportation network was well on its way.
Today, maritime transportation contributes to one-quarter of US GDP, or some $5.4 trillion. No global supply chain is independent of maritime transport, and most, in fact, are existentially dependent on it. Outside the United States, the sea and ports worldwide moved around 80 percent of global trade by volume and over 70 percent of global trade by value. Global maritime trade continues to gather momentum; in 2018, the industry expanded by 4 percent globally—the fastest growth in five years.

The maritime transportation sector also is crucial for the success of other critical infrastructure sectors —specifically, the security of global energy systems. In 2016, more than 61 percent of the world's total petroleum and other liquid energy supply was moved through sea-based trade. Maritime shipping as a form of transportation is essential for bulk transport of these raw materials due to the sheer volume of goods that must be moved and the competitive price point the MTS offers.   Maritime trade is essential for supplying fuel to the global economy.
A critical part of the United States' national security is the ability to project power across the oceans; the shipping industry is a crucial cog of this wheel. Sealift—the ability for large-scale transportation of troops, supplies, and equipment by sea—is the basis of US military power projection, handling more than 90 percent of the US Department of Defense's (DOD) wartime transportation requirements.   Sealift is the largest provider of strategic mobility, a driver of economic prosperity during wartime, and a key contributor to the US military's global operating model. Sealift has manifested in variety of ways, including shipping essential supplies such as oil and natural gas (ONG) to the Middle East in support of Operation Iraqi Freedom, or providing humanitarian assistance to the Philippines after brutal natural disasters, such as Typhoon Haiyan. The central role of sealift in enabling a diverse set of global operations—and the need to use maritime transportation to enable agile and strategic activity below the level of armed conflict, such as freedom of navigation operations, makes maritime security essential to US national security.

The Merchant Marine Act of 1920—better known as the Jones Act—further defines the relationship between the MTS and national security. Signed into law just after World War I, the Jones Act seeks to promote and maintain the US merchant fleet to ensure that the country will have sufficient merchant sealift capacity in the event of a conflict or an incident requiring the transport of large volumes of personnel and materiel. Among other provisions, it stipulates that any vessels transporting passengers or goods—even liquefied natural gas (LNG)—between US ports must be built, owned, flagged, and crewed by US citizens or permanent residents. A century since the Jones Act's enactment, there are fewer than two hundred vessels that fulfill the statute's criteria, many of which rely on subsidies from the government to maintain that capacity.

Despite being one of the largest producers of natural gas, the United States is restricted by the Jones Act from shipping its own LNG to domestic ports on noncompliant vessels.

More broadly, maritime trade also plays a key role on the global geopolitical stage for allies and potential adversaries. The United States is dependent on the ability to import goods from its allies via maritime transport: around 90 percent of US total imports arrive by sea. China, a near-peer rival of the United States, is acutely dependent on imports of oil and key resources such as iron to fuel its growing economy—goods that are almost exclusively transported through maritime trade routes. Maritime security is of vital interest to China, as the geography of the Asia-Pacific region and, specifically, the strategically significant straits of Malacca and Singapore represent some of the most critical choke points and active trade routes in the world and global maritime traffic has increasingly concentrated on these geostrategic choke points. All of these factors have driven industry players to boost efficiency, automation, and remote management, in a word, more technology. The result however is widespread adoption of software and hardware without adequate corresponding management of the growing specter of cyber risk.

COMPLEXITY BEGETS INSECURITY

Much like many other critical infrastructure industries, operational efficiency and profit drive maritime transportation. That drive has caused a shift toward an even more complex environment—and complexity begets insecurity. As the size of the global economy and its reliance on maritime activity have accelerated, the maritime transportation sector has had to scale up its operations. Over the last fifty years, the size and capacity of cargo ships have increased 1,500 percent. In many ways, this dramatic scale-up has been essential for the industry. It has allowed for an exponential increase in sea trade and has driven prices down internationally. This rapid increase in size, however, has resulted in ships, and the MTS more broadly, becoming more complex.

The MTS is not monolithic. It’s a “system of systems” composed of ships and ports, but also the shipping lines, manufacturers, intermodal transport operators, cargo and passenger handlers, vessel traffic control, and maritime administrators. Each of these is itself a system of systems with complex internal and external dependencies. While all ports have similarities, they vary in their ownership and tenant models, cargo- and passenger-handling capabilities, mix of civilian and military vessels, jurisdictional authorities, and more. Similarly, all ships have some common functions, but are fundamentally different in areas such as operation, cargo and passenger capabilities, and crew requirements. Applying regulations to vessels is often complicated by the fact that one’s country of registration, ownership, and management might all be different, thus often requiring the coordination of several countries when adjudicating an incident.

Cybersecurity needs to be implemented and practiced by people engaged in all maritime activities—not just IT experts. The users of the MTS are a mixed lot: they work for a wide variety of organizations, play myriad roles, and have varied professional backgrounds and experiences. A given body of water might see any combination of commercial, law enforcement/public safety, military, cargo, passenger, recreational, maintenance, and other types of boats—not to mention offshore drilling or wind platforms, weather and navigation buoys, and sea-based communication platforms.

For years, the maritime sector developed and deployed unique software and hardware, inherently limiting their connectivity and risk exposure. However, the interconnected and data-rich world of the twenty-first century has provided ship and port owners and operators with an opportunity to integrate more ubiquitous IT systems with OT ones. These changes have led to increased automation, digitalization, levels of operational efficiency, and of course, better margins for owners and operators. Despite the MTS's increasing deployment of OT and interconnected technology, from ships to rigs to ports, the sector has not proportionally increased its focus on cybersecurity.

Existing cybersecurity efforts in the MTS prove that it is tough to securely design, develop, and operate a fully connected environment—and even more so when these environments look different on a ship-to-ship and port-to-port basis. The MTS's increased reliance on converging OT and IT systems has introduced new vulnerabilities and expanded the attack surface in the maritime environment—yet the focus and resources devoted to combatting these new threats still largely lags this development. In the integrated MTS, cybersecurity is only as good as the weakest link. It is critical that all links in the MTS logistical chain collaborate in establishing robust programs, properly training personnel, and maintaining the operational efficiency necessary for all parts to work as one. However, this is easier said than done.

The consequences of this disconnect—the shortfall in cybersecurity investment compared to the increase in automation and digitization—have become increasingly clear in recent years. This often manifests itself similarly to other industries. Ransomware and phishing, two of the more common tactics and means of compromise globally, exist extensively throughout the MTS. In fact, all four of the world's largest maritime shipping companies—A. P. Moller-Maersk (Maersk, as it is known, is part of the A. P. Moller Group), China Ocean Shipping Company (COSCO) Group, and Mediterranean Shipping Company (MSC)—have been hit by significant cyberattacks since 2017. Maersk, whose business operation systems were ravaged when the NotPetya malware spread from an infected Ukrainian tax-preparation software called MeDoc, spent more than $300 million to return to full operations after ten days of repair and remediation. A reported 400-percent increase in maritime cyberattacks during 2020, along with a 900-percent increase in attacks targeting ships and port systems over the prior three years, point to a maritime industry in the crosshairs of malicious cyber actors. Despite this, the industry and its regulators have only slowly begun to move toward meaningful and systemic change.

Given the complexity and segmented ownership of the organizations comprising the MTS, as well as the range of threats, there is no single authority or cybersecurity model that easily applies to the entire industry. A more modular approach is needed to take a collective understanding of vulnerabilities and threats, and segment the MTS into individual systems that can support one another and/or leverage gains in other systems, and be addressed by policy makers. The approach ultimately must be holistic; even if every component of the MTS was cyber secure, the interconnection of the subsystems might not result in a secure whole. A better understanding of the cybersecurity threat landscape, coupled with a segmented view of MTS infrastructure, will be necessary to build a secure maritime domain. This approach will allow developers, policy makers, owners, and regulators to match the best policy levers with particular maritime systems, and achieve better management of cyber risk across the entire MTS.

THREATS

The elements, pirates, and rival powers have challenged the maritime shipping industry for thousands of years. As the industry expands in size and integrates new technologies for added efficiency, the volume of potential threats, and the consequences of potential disruption increase exponentially.

In addition to the implementation of new and insecure technology, in the last several years new problems and worsening effects have challenged the maritime industry in different ways. In early 2021, a Maersk vessel lost 260 containers overboard—about 2 percent of its cargo—when the ship lost propulsion for less than four minutes in heavy seas. This was not an isolated incident; both MSC and NYK Ship management (NYKSM) have each had significant and comparable incidents since late-2020. Over the last decade, the World Shipping Council estimated that an average of 1,382 containers have been lost overboard annually. While not all of these losses are linked to cyber incidents, they illustrate how much risk exists in the ecosystem, and how the increased scale and complexity of the MTS have given rise to new concerns.

The COVID-19 pandemic is evidence of the effects that a massive disruption can inflict on the MTS. The pandemic challenged the maritime industry with port closures, a new and shifting demand landscape, significant supply-chain disruptions, and operational questions around health and safety. As a result, for the first time in decades, global maritime trade actually dropped 4.1 percent in 2020. No doubt, the pandemic also will have long-term effects on the industry that are hitherto impossible to quantify. COVID-19 forced states to think differently about their international relationships and trading patterns. The economic and security consequences of such a large-scale disruption shocked many—and proved how unprepared the MTS is for such systemic challenges.

The most recent and probably most notable single-event example of an MTS-wide disruption occurred when Ever Given, one of the largest commercial container ships in the world, got stuck shortly after entering the Suez Canal in March 2021, blocking through traffic on one of the world's busiest waterways. The vessel, at 1,300 feet (400 meters) and nearly 221,000 gross tons, was stuck for more than six days and took several days of work from one of the world's best salvage teams, a fortuitous high tide, and a dash of luck to un-wedge. Although the cause of the incident is believed to be a combination of heavy winds, the ship's speed, and the vessel's rudder size/alignment rather than a cyber-attack, the mishap caused global economic disruption. With 13 percent of global trade passing through it every year, the narrow Suez Canal is one of the most strategically important choke points in the world. The resultant blockade of Suez Canal traffic held up $9.6 billion in goods. Once unstuck, the price to "refloat" the ship landed at $900 million, to be followed by a dispute over financial damages that ended in the seizure of Ever Given for nearly four months by Egyptian authorities.

The Ever Given incident illustrates the scale of disruption that a cyber-incident could have on global shipping, especially in geostrategic choke points. It also exemplifies the complexity and interconnectedness of the global maritime system. Ever Given was owned by a company in Japan, operated by a container shipping firm based in Taiwan, managed by a German company, registered in Panama, and crewed by twenty-five Indian nationals. The complex, interconnected, and multinational nature of the MTS makes coordination challenging and finger pointing around incidents common—but also provides the industry with a unique opportunity to leverage systemic and global change if handled correctly.

There are precedents for high-consequence cyber events causing disruption on the MTS, including in the United States. In November 2020, the Port of Kennewick was hit by sophisticated ransomware attack that forced operators to rebuild the Washington state port's digital files from offline backups. This was not an isolated incident, but emblematic of a larger trend.

The cyber-threat landscape in the MTS is similar to that of other critical infrastructure sectors. Global Positioning System (GPS) and Automatic Identification System (AIS) jamming and spoofing, attacks on less-than-secure OT and industrial control-system (ICS) devices, human targets, myriad shipboard information and communications technology (ICT) systems, are just some of the vectors that adversaries can and will use to attack the MTS. Ransomware, software supply-chain attacks, and social engineering are a few common tactics, techniques, and procedures (TTP) that have been used against the MTS. Potential targets and victims throughout the MTS include ships, ports, passenger and cargo shipping lines, shipbuilders and maritime manufacturers, and others. It is a complex and extraordinarily dynamic ecosystem that is difficult to defend. Cyberattacks represent an existential threat to the contemporary maritime industry, the smooth operation of which underpins modern society.

ATTACKERS AS DIVERSE AS THE MTS: PIRATES TO OWNERS

The MTS's vulnerability to cyberattacks and its significance to US national security and economic stability have drawn from the woodwork an array of adversaries' intent upon wreaking harm on the ecosystem.

Just as the MTS is not monolithic, neither are those posing a threat to it. There is no single profile of a threat actor and motivation for attacking maritime cyber systems. Sun Tzu's well-known saying about knowing thy enemy applies here: "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." Understanding where your risk is concentrated and who may look to exploit that risk are essential steps to securing an organization's systems.

Attackers in cyberspace generally fall within the following categories based largely on intent.

1. **Cybercriminals:** Like criminals in the physical domain, cybercriminals are after financial or other tangible rewards; they are not ideologues, they want the cash. Cybercrime costs the global economy more than $1 trillion annually. Cybercriminals in the MTS engage in cyber fraud and are behind most ransomware campaigns.
2. **Cyber activists/Hacktivists:** Philosophy, politics, social movements, and other nonmonetary goals motivate this group of threat actors. Typical tactics of hacktivists include defacing websites, launching protests on social media, and conducting acts of cyber vandalism; while often criminal in nature, the intent is rarely financial.
3. **Terrorists:** The use of cybersecurity capabilities by a traditional terrorist actor could mirror an act of terrorism in real space—a violent criminal action, meant to intimidate or

cause fear—and be motivated by political aims. This fear could directly, or indirectly, yield disruption with significant economic effects. Terrorist groups also often engage in cyberattacks with financial motivations to fund other operations and help support recruitment.

4. **State-sponsored entity:** State-sponsored entities: These actors often report to or receive support from nations or states. Acts of financial, industrial, political, and diplomatic espionage in cyberspace are the most common objectives for this type of entity. Intellectual property (IP) theft, in particular, costs the global economy more than $2 trillion annually by some estimates.
5. **State actor:** Such actors have the resources and capabilities to conduct nuanced and sophisticated cyber operations. Although the most prominent state actors targeting the MTS are Russia and China, both Iran and North Korea have proven capable of attacking numerous industrial sectors internationally. These operations normally work to advance strategic goals. There is no international consensus on a definition of "an act of war" in cyberspace and, therefore, it is unclear how defense treaties in traditional spaces influence hostile activities in cyberspace.

While an understanding of the distinctions among threat actors can be useful in considering how to protect specific systems, a strict categorization of any given cyberattack is often difficult because the lines differentiating these actors blur during any dynamic event. Attribution is often a challenging and lengthy process, and results can sometimes be tentative at best. Many criminal organizations in cyberspace, for example, have nation-state sponsors yet their actions are not considered state-sponsored.

Attackers have their own motivations, levels of capability, technological and financial resources, opportunities, time frames, and intents. The primary threat actors that have demonstrated a high capacity and willingness to conduct operations against the MTS and related critical infrastructure sectors fall within two categories: cybercriminals and state-sponsored actors. There are thin boundaries between these categories, given that some state-sponsored groups also operate within well-known cybercriminal networks.

The main focus of cybercriminals is most often monetary gain. They target well-known organizations with large attack surfaces, prey on employees' lack of cyber awareness, and aim for large monetary rewards. To accomplish these ends, ransomware has become one of the most common and public forms of cyberattacks against MTS targets. Ransomware is used to paralyze a victim organization by encrypting its data and requesting a ransom, often to be paid into a pseudonymous cryptocurrency wallet. Most ransomware attacks are conducted by criminal organizations for their own profit, or to fund criminal and terrorist activities in conventional space. Some other monetary motivations include reselling access to the infrastructure, information obtained, or compromised computers on the dark-net, a network using the Internet that requires permission or special software.

Cyberespionage operations targeting the maritime community also are common, primarily in the form of intelligence gathering and Internet Protocol (IP) theft. Cyberespionage represents a middle ground of activity that can be valuable for both criminals and state actors. In March 2019, for example, Chinese state-sponsored hackers reportedly targeted universities around the world, as well as the US Navy and industry partners, in order to steal maritime technology. China also has an ownership and/or operational presence at dozens of major ports around the world, providing a wide capability for information gathering on ports, vessels, and cargoes. Obtaining this type of access to MTS infrastructure can provide information of strategic significance regarding MTS cyber-physical security, information-system vulnerabilities, and operational information. Furthermore, adversaries may consider breaching a network using zero-day attacks to maintain persistent access to MTS networks to affect or influence the infrastructure operations at the right time.

More sophisticated, state-sponsored attacks are just starting to find their way into the MTS, with incidents such as the May 2020 cyberattack by Israel on Iran's Shahid Rajaee port in Bandar Abbas in response to Iran's cyberattack on Israel's water-supply system the previous month.[37] Directed spoofing and jamming attacks on global positioning, navigation, and timing (PNT) systems by Russia, China, Iran, and North Korea are additional threats affecting the MTS as well as other transportation sectors.

FRAMING THE CHALLENGE

It is imperative to establish at the outset that there is no silver bullet for maritime cybersecurity. A history of old shipboard technology has been retrofitted to an era of interconnectivity, which has created a fractured and vulnerable maritime environment.

This report is intended to deliver a more complete and operational plan to better protect the MTS by focusing on building upon, broadening, and deepening the priorities put forward by the NMCP. The US government took an important first step in December 2020 when it released the National Maritime Cybersecurity Plan. The plan aims to "buy down the potential catastrophic risks to national security and economic prosperity caused by MTS operators' increasing reliance on IT and OT, while still promoting maritime commerce efficiency and reliability." To achieve this goal, the plan focuses on three key principles: risks and standards, information and intelligence sharing, and creating a maritime cybersecurity workforce. The plan represents a significant step in the right direction and calls attention to many of the critical risks outlined in this report. However, it lacks specificity on how to implement these three principles. This report started by highlighting both the significance of the MTS and some of the most common and consequential threats to the MTS. Now it pivots to discuss major drivers of risk to the MTS and three maritime life cycles—ships, ports, and cargo—and the key programs, vulnerabilities, and stakeholders in each. These sections are explicitly intended to extend the NMCP and identify areas of risk and potential progress for policy makers and industry. The final section builds on the points of leverage identified in these three life cycles and offers specific recommendations to the United States, US allies, and the private sector to cooperatively reduce and better manage the system's cybersecurity risks.

EXPLORE THE FULL REPORT

This *Introduction* is part of a larger body of content encompassing the entirety of *Raising the colors: Signaling for cooperation on maritime cybersecurity*— use the buttons below to explore this report online: **Https://www.Introduction: Cooperation on maritime cybersecurity - Atlantic Council**

Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends, CISA & FBI, 22NOV2021

As Americans prepare to hit the highways and airports this Thanksgiving holiday, CISA and the Federal Bureau of Investigation (FBI) are reminding critical infrastructure partners that malicious cyber actors aren't making the same holiday plans as you. Recent history tells us that this could be a time when these persistent cyber actors halfway across the world are looking for ways—big and small—to disrupt the critical networks and systems belonging to organizations, businesses, and critical infrastructure.

There are actions that executives, leaders, and workers in any organization can take proactively to protect themselves against cyberattacks, including possible ransomware attacks, during the upcoming holiday season—a time during which offices are often closed, and employees are home with their friends and families. Although neither CISA nor the FBI currently have identified any specific threats, recent 2021 trends show malicious cyber actors launching serious and impactful ransomware attacks during holidays and weekends, including Independence Day and Mother's Day weekends.

CISA and the FBI strongly urge all entities–especially critical infrastructure partners–to examine their current cybersecurity posture and implement best practices and mitigations to manage the risk posed by cyber threats. Specifically, CISA and the FBI urge users and organizations to take the following actions to protect themselves from becoming the next victim:

- Identify IT security employees for weekends and holidays who would be available to surge during these times in the event of an incident or ransomware attack.
- Implement multi-factor authentication for remote access and administrative accounts.
- Mandate strong passwords and ensure they are not reused across multiple accounts.
- If you use remote desktop protocol (RDP) or any other potentially risky service, ensure it is secure and monitored.
- Remind employees not to click on suspicious links, and conduct exercises to raise awareness.

Additionally, CISA and the FBI recommend maintaining vigilance against the multiple techniques cybercriminals use to gain access to networks, including:

- Phishing scams, such as unsolicited emails posing as charitable organizations.
- Fraudulent sites spoofing reputable businesses—it is possible malicious actors will target sites often visited by users doing their holiday shopping online.
- Unencrypted financial transactions.

Finally—to reduce the risk of severe business/functional degradation should your organization fall victim to a ransomware attack—review and, if needed, update your incident response and communication plans. These plans should list actions to take—and contacts to reach out to—should your organization be impacted by a ransomware incident. **Note**: for assistance, review available incident response guidance, such as the Ransomware Response Checklist in the CISA-MS-ISAC Joint Ransomware Guide, the Public Power Cyber Incident Response Playbook, and the new Federal Government Cybersecurity Incident and Vulnerability Response Playbooks.

CISA and the FBI urge users and organizations to take these actions immediately to protect themselves against this threat. For a comprehensive overview, see the joint Cybersecurity Advisory Ransomware Awareness for Holidays and Weekends. For more information and resources on protecting against and responding to ransomware, visit StopRansomware.gov, a centralized, whole-of-government webpage providing ransomware resources and alerts.

HOW YOU CAN HELP PROTECT CALIFORNIA

State, local, and tribal governments, non-governmental organizations and the private sector can partner with the Cal-CSIC by registering to receive Alerts and Advisories, sharing IOCs and cyber incident reports, and connecting to the California Automated Indicator Exchange.

- Email the Cal-CSIC to learn more about sharing of IOCs and connecting to the California Automated Indicator Exchange at calcsic@caloes.ca.gov.
- Report cyber incidents to the Cal-CSIC at (833) REPORT-1 or calcsic@caloes.ca.gov.

IMPORTANT NOTIFICATION CONTACT INFORMATION

Companies, facilities or vessels required to have a Marine Transportation Security Act (MTSA) security plan must report suspicious activities or breaches of security to the Coast Guard's National Response Center (NRC), or **cyber-attacks** to the National Cybersecurity and Communications Integration Center (NCCIC):

- (NRC) Phone 1-800-424-8802 or direct phone line at 202-372-2428
- (NRC) Fax 202-372-2920
- (NRC) Web: http://www.nrc.uscg.mil/
- (NCCIC) at 888-282-0870

After calling the NRC/NCCIC, call the Captain of the Port, San Francisco, at 415-399-3530.

Other agencies you may want to consider reporting to are:

California Cybersecurity Integration Center – (916) 636-2997 and CalCSIC@caloes.ca.gov

The Federal Bureau of Investigation (FBI) should be notified of cyber security breaches:

- FBI Headquarters – threats and crime reporting: https://tips.fbi.gov/
- San Francisco Office – 415-553-7400 (san.francisco@ic.fbi.gov)
- Sacramento Office – 916-841-9110 (http://www.fbi.gov/sacramento)
- Internet Crime Center – http://www.ic3.gov/complaint/default.aspx
- InfraGard Website – https://www.infragard.org/

U.S. COAST GUARD HOMEPORT PORTAL

The U.S. Coast Guard maintains links to various sources of maritime security information on its HOMEPORT information portal. The link to U.S. Coast Guard's HOMEPORT maritime security information portal is:

- Web – http://www.homeport.uscg.mil/

CUSTOMER FEEDBACK

How are we doing? Please send feedback about this newsletter to Mr. Paul Martin, USCG Sector San Francisco, at:

- E-mail – Paul.R.Martin@uscg.mil

Note: articles appearing in this newsletter were submitted by port stakeholders or downloaded from public websites and posted without editing. If you have an article to post, please provide the article to Mr. Martin at the above e-mail address. This newsletter is a quarterly publication and generally published shortly before a meeting of the Northern California Area Maritime Security Committee. **This newsletter is for public information purposes only**; articles containing proprietary, sensitive but unclassified, or classified information will not be accepted. The U.S. Coast Guard reserves the right to decide which articles are published in this newsletter.