NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
January 2017 (edition 2017-1)

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 news letter will be e-mailed to members of the Northern California Area Maritime Security Committee, posted on the Coast Guard's HOMEPORT portal and may be posted by the San Francisco Marine Exchange.

TABLE OF CONTENTS

ARTICLE SUMMARIES

- **ABS Awarded a Maritime Cybersecurity Contract** – American Bureau of Shipping has been awarded a two-year research program focused on defining the future of cybersecurity for the maritime industry.
- **Cyber Breaches Are a Top Risk, Shipping Execs Say** – Shipping industry executives say the increased security threat from cyber and data privacy breaches is the number one risk to its sector, according to a new ranking released today by Willis Towers Watson (NASDAQ: WLTW), a leading global advisory, broking and solutions company.
- **Rough Waters Ahead for Port Security** – This past August, the US Coast Guard published its long-awaited final rule on TWIC readers, which requires a range of covered facilities and vessels to install electronic TWIC readers within the next two years.

- **Be Cyber Aware at Sea' Campaign** – The 'Be Cyber Aware at Sea' campaign to help raise awareness of cyber threats and risks to ship owners and offshore energy suppliers through an industry messaging initiative which includes posters, short educational films, guidance booklets for on board crew members and a bespoke maritime cyber training program.
- **GovRAT Malware** – The GovRAT Malware platform has been upgraded.
- **DDoS Attacks a Military Tool to Shut Down Internet** – Security researcher Bruce Schneier spotted a series of DDoS attacks which may be part of a larger effort to learn how to take down the internet on a national or even global scale. The attacks targeted major companies that provide the basic infrastructure for the internet and the incidents seem to appear to have probed the companies' defenses to determine how well they can protect themselves.
- **Industry Employee Tip Card** – excerpt from a DHS cybersecurity help pamphlet.
- **Industry Leadership Tip Card** – excerpt from a DHS cybersecurity help pamphlet.
- **Cyber Crime Poses Threat to Autonomous Shipping** – an article about how the threat posed by cyber-attacks are affecting research into autonomous ship research and development.
- **The Year in Cyber Crime** – a compilation of this year's threats & forecasts (attached).

MAIN ARTICLES

FBI (10/16) ABS Awarded a Maritime Cybersecurity Contract, 10 October 2016, Online Source

ABS Contracted for 2-Year Maritime Cybersecurity Research Project - International classification society the American Bureau of Shipping has been awarded a research by the U.S. Maritime Security Center to conduct a two-year research program focused on defining the future of cybersecurity for the maritime industry. Participants in the study will include U.S. Department of Homeland Security (DHS) Center of Excellence, led by Stevens Institute of Technology, and the Department of Defense. "Cybersecurity incursions and threats to the Marine Transportation System (MTS) and port facilities throughout the country are increasing," says Dr. Hady Salloum, Director of MSC. "This research project will support the missions of the DHS Center of Excellence and the U.S. Coast Guard to address these concerns and vulnerabilities and will identify policies and risk management strategies to bolster the cybersecurity posture of the MTS enterprise."

FBI (10/16) Cyber Breaches Are a Top Risk, Shipping Execs Say, October 2016, Ben Abraham

Shipping industry executives say the increased security threat from cyber and data privacy breaches is the number one risk to its sector, according to a new ranking released today by Willis Towers Watson (NASDAQ: WLTW), a leading global advisory, broking and solutions company.

According to Willis Towers Watson's Transportation Risk Index the second- and third-most pressing risks affecting the shipping sector are globalization of the customer base, and third-party security vulnerabilities. Failure of critical IT systems, change in demand due to macroeconomic conditions and dependence on third-party suppliers are ranked fourth, fifth and sixth in the index, respectively.

"Our survey found the prolonged economic struggles of most shipping companies have made the maritime sector more sensitive to risk than other modes of transport," said Ben Abraham, head of Willis Towers Watson's Marine practice.

"Maritime transport providers perceive cyber and data privacy breaches as their top risk. But shipping companies are also heavily exposed to globalization. Nowhere is this more apparent than with the bankruptcy of South Korea's Hanjin Shipping. Its demise, stranding more than $14 billion in goods at sea, is a case study of the industry's interdependence."

The risk ranking is based on interviews with 63 C-suite executives across the shipping sector globally, which includes ship owners, port and terminal operators and cruise operators. The respondents were asked to rank 50 risks according to their potential impact and how difficult each one would be to manage.

"Global shipping companies clearly face a complex, interconnected risk environment. Understanding your risks and knowing how to respond provide a competitive advantage," added Abraham.

FBI (10/16) Rough Waters Ahead for Port Security, October 4, 2016, Ben Lerner

The anniversary of 9/11 has historically been not only a time to mourn those we lost on that day, but also a time to reflect on the extent to which we've made meaningful progress on stopping the next catastrophic attack. That reflection has included assessing the present state of transportation security, with aviation security understandably foremost on experts' minds. On the heels of the recent discovery of five explosive devices at an Elizabeth, New Jersey train station, and with the attack on a Brussels rail station last March still resonating, the safety of rail transportation has also been a prominent feature of that discussion in recent weeks, as it ought to be.

Against this backdrop, is another anniversary -- the October 12th sixteenth anniversary of the attack on the USS Cole, during which Al Qaeda operatives rammed an explosives-laden motorboat into the Navy vessel, which at the time was docked for refueling in Aden, Yemen. Seventeen sailors were killed. On that day, terrorists acted on their interest and capability to attack a significant maritime target using asymmetric tactics – that, and their record for targeting the transportation sector, should be taken as indicators that they remain interested in maritime attacks, likely now with a view to domestic targets including civilian ships and the ports servicing both passengers and freight.

Sixteen years after the USS Cole, despite some important progress in the past decade, troubling vulnerabilities persist in the maritime domain. In 2009, it became mandatory that individuals requiring unescorted access within regulated US maritime facilities and vessels possess a biometric security credential (with name, expiration date, photo and two fingerprints), known as the Transportation Worker Identification Credential, or TWIC, issued by the Department of Homeland Security (DHS).

This past August, the US Coast Guard published its long-awaited final rule on TWIC readers, which requires a range of covered facilities and vessels to install electronic TWIC readers within the next two years. The intent of requiring an electronic TWIC reader is to prevent the use of forged credentials. Weeding out forged TWICs is eminently sensible, but it won't do much good if the TWIC was legitimately issued to a malevolent actor in the first place. DHS's Inspector General (IG) recently issued a report indicating that there are concerning flaws in the Transportation Security Administration's (TSA) TWIC issuance process – one line in the IG's audit that especially stands out is that, "Adjudicators may grant TWICs even if questionable circumstances exist."

While the insider threat to maritime targets requires continued vigilance, the outsider threat is no less salient and the trend towards innovation is cause for concern. Drug cartels have been moving large amounts of narcotics into the United States on homemade "narco submarines," which since their debut in 1993 have become more sophisticated in their ability to evade detection by radar or sonar. Given previous and ongoing cooperation between drug cartels and terrorist organizations, it is entirely feasible that the cartels would share this technology with those who may want to use it to deliver, or act as, an underwater improvised explosive device (IED). Recognizing this threat, the Department of Defense is already working with the private sector to design and field a remotely operated underwater vehicle to detect and disarm underwater IEDs.

Then there's the threat of intrusion from afar in the form of cyberattacks on our port operations and maritime vessels. Port and maritime operations have become highly automated in previous years, adding to economic efficiency while simultaneously creating opportunities for hackers to infiltrate the system and potentially cause severe damage. In addition to the economic consequences of such breaches, there is a significant public safety concern as well – Congress has already noted that hackers could cause the release of dangerous chemical cargoes passing through American ports, many of which are near populated areas, and others have warned that today's large ships are highly reliant on automated GPS navigational systems, the compromise of which could result in intentional collisions. The US Coast Guard and Congress have both been taking steps to address the threat of cyber-attacks on maritime assets, but it remains to be seen whether such processes will stay ahead of that threat, or lag behind it.

To make matters more challenging, we are not adequately bolstering our frontline defense. The American Association of Port Authorities (AAPA) testified before Congress last summer that in fiscal year 2015 when Customs and Border Protection was given budget authority to hire 2,000 staff, fewer than 20 officers of which were assigned to ports. AAPA also observed that directors of port security in the United States are not routinely given security clearances to receive briefings from the federal government on the threat outlook for their respective ports.

AAPA had high praise for the Federal Emergency Management Association (FEMA) Port Security Grant Program, but that program has seen steady reductions in funding during the past several years – from a height of over $388 million in FY 2008, down to today's FY 2016 funding level of $100 million, a roughly 74 percent decrease. As it currently stands, 80 percent of the TSA $7.4 billion budget goes towards aviation security.

There are efforts underway in Congress to put more transportation security focus on the maritime domain. Senators John Thune (R-SD) and Bill Nelson (D-FL) recently introduced legislation to require TSA to provide an assessment on threats to surface and maritime transportation, and to implement a risk-based strategy to address those threats, using a risk-based budget plan.

Thune's bill is the Surface Transportation and Maritime Security Act (S.3379).

The House version of the FY 2017 Intelligence Authorization Act contains language requiring DHS to submit a report to Congress on the threat of cyber-attacks on US ports, while the House has already passed legislation to direct DHS to create voluntary guidelines for ports to facilitate reporting on cyber threats.

At the moment, however, these initiatives are on hold.

Sixteen years after the USS Cole, the port/maritime space remains a target. Now is the time for policymakers, at all levels of government, to redouble their efforts to better secure it.

Ben Lerner is Vice President for Government Relations with the Center for Security Policy.

FBI (10/16) Be Cyber Aware at Sea' Campaign, October 2017, Maritime Security Review, Online Article

JWC International a leading provider of Maritime & Offshore Cyber Security Training Solutions have launched the 'Be Cyber Aware at Sea' campaign to help raise awareness of cyber threats and risks to ship owners and offshore energy suppliers through an industry messaging initiative which includes posters, short educational films, guidance booklets for on board crew members and a bespoke maritime cyber training program. It was recently reported that more than 80% of offshore (situated at sea) Cyber, Information Technology (I.T) and Operational Technology (O.T) security breaches are as a direct result of human error. The International Maritime Bureau (IMB) also recently reported that cyber-crime at sea was on the rise and ship owners should be aware of the consequences of not implementing risk mitigation measures.

FBI (10/16) GovRAT Malware, InfoArmor, October 2016

A tough-to-detect malware that attacks government and corporate computers has been upgraded, making it more aggressive in its mission to steal sensitive files, according to security firm InfoArmor. Last November, InfoArmor published details on GovRAT, a sophisticated piece of malware that's designed to bypass antivirus tools. It does this by using stolen digital certificates

to avoid detection. Through GovRAT, hackers can potentially steal files from a victim's computer, remotely execute commands, or upload other malware to the system. Earlier this year, however, the makers of GovRAT came out with a second version, according to a new report from InfoArmor. The malware features an additional function to secretly monitor network traffic over the victim's computer -- something with scary consequences.

FBI (10/16) DDoS Attacks a Military Tool to Shut Down Internet, SC Magazine, Bruce Schneier, September 15, 2016

Security researcher Bruce Schneier spotted a series of DDoS attacks which may be part of a larger effort to learn how to take down the internet on a national or even global scale. The attacks targeted major companies that provide the basic infrastructure for the internet and the incidents seem to appear to have probed the companies' defenses to determine how well they can protect themselves, according to a Sept. 13 blog post.

Schneier said he is unable to give details concerning which companies were targeted because he spoke with the companies under anonymity, but said the attack rate has increased in the last two years and that his findings are supported by a Verisign DDoS trends report. Schneier told SCMagazine.com he believes the attacks are part a foreign cyber organization doing military recon activities. The attacks are believed to be from China, but that being said Schneier said he is hesitant to point the blame at anyone. So far, the targeted companies have been able to defend themselves, but when it comes to actually being able to take down the internet, Schneier said, “it does seem you can do it for small amounts of time but not permanently.”

Some other experts agree. Several countries have a history of using DDoS attacks to target the U.S. and other nations so it's safe to say that if taking down the internet will improve one's position as a world power, someone will try to do it, Plixer CEO Michael Patterson told SCMagazine.com via emailed comments. “Consider the past attacks on our utilities and our 911 system and you can begin to appreciate the possibility of a combination of attacks that would certainly be possible with DDoS technologies,” Patterson said. “Our government needs to develop and implement a full-scale back-up in the event that any one of these world players are successful in taking down the Internet.”

Patterson said so much of the U.S. economy depends on the internet that its critical to have an alternative communication and digital plan in place in case something happens. However, some industry pros expressed doubt that an attacker would be able to carry out such a large-scale attack. While the size, duration, and sophistication of DDoS attacks continue to grow, a complete shutdown is unlikely, Tim Matthews, Imperva Incapsula VP of marketing, told SCMagazine.com via emailed comments. “Attacks might present temporary regional slowdowns – and annoy customers – but certainly not cause a global Internet blackout, as Mr. Schneier suggests,”

Matthews said. “And with proper DDoS protections in place, most attacks like these would be stopped in their tracks.”

DHS (11/16) Industry Employee Tip Card, Department of Homeland Security, Online Source, Nov 2016

All employees play an important role within their organization. Each person must employ proper cybersecurity practices to ensure that all work-related information stays safe and secure. When each person makes a conscious and proactive effort to learn about cybersecurity, they enhance the company’s ability to guard and protect the organization from vulnerabilities.

DID YOU KNOW? A combined 92 percent of human resource professionals said increased vulnerability of business technology to attack or disaster will have an effect on the U.S. workplace in the next five years.

SIMPLE TIPS
1. Read and abide by your company’s Internet use policy.
2. Make your passwords complex. Use a combination of numbers, symbols, and letters (uppercase and lowercase).
3. Change your passwords regularly (every 45 to 90 days).
4. Don’t share any of your user names, passwords, or other computer or website access codes.
5. Only open emails or attachments from people you know.
6. Never install or connect any personal software or hardware to your organization’s network or hardware without permission from your IT department.
7. Make electronic and physical back-ups or copies of all your most important work.
8. Report all suspicious or unusual problems with your computer to your IT department.

US-CERT.gov

The United States Computer Emergency Readiness Team (US-CERT) has numerous tips and resources on topics like choosing and protecting passwords, email attachments, and safely using social networks

FBI.gov

The Federal Bureau of Investigation leads the national effort to investigate high-tech crimes, including cyber-based terrorism, computer intrusions, online sexual exploitation, and major cyber-crimes.

CyberCrime.gov

Cybercrime.gov is the Department of Justice component responsible for implementing national strategies in combating computer and intellectual property crimes worldwide.

IF YOU'VE BEEN COMPROMISED

• Report it to your manager or contact the IT or legal department to report the incident.
• Keep and record all evidence of the incident and its suspected source.
• Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov, if applicable.
• Report fraud to the Federal Trade Commission at www.onguardonline.gov/file-complaint, if applicable.
• If someone has had inappropriate contact with you or a colleague, report it to www.cybertipline.com and they will coordinate with the FBI and local authorities. You can also report it to the Department of Justice at www.justice.gov/criminal/cybercrime/ reporting.html.

URL = https://www.dhs.gov/sites/default/files/publications/Industry-Employee-Tip-Card.pdf

DHS (11/16) Industry Leadership Tip Card, Department of Homeland Security, Online Source, Nov 2016

As a business leader, it is important to constantly be cyber-aware and incorporate cyber safety into your business strategy. Employees will look to leadership for best practices and proper execution of safe cybersecurity habits. By practicing healthy cybersecurity hygiene now, your business will have a better chance of avoiding compromised systems and lost profits.

DID YOU KNOW?
• The yearly cost of cyber-crime per organization spanned a range of $1.3 million to $58 million.1
• The cost of cyber-crime increased 26 percent, or $2.6 million from 2012 to 2013.

SIMPLE TIPS

1. Implement a layered defense strategy that includes technical, organizational, and operational controls.
2. Establish clear policies and procedures for employee use of your organization's information technologies.
3. Coordinate cyber incident response planning with existing disaster recovery and business continuity plans across your organization.

4. Implement technical defenses, such as firewalls, intrusion detection systems, and Internet content filtering.
5. Update your anti-virus software often.
6. Follow your organization's guidelines and security regulations.
7. Regularly download vendor security patches for all of your software.
8. Change the manufacturer's default passwords on all of your software.
9. Encrypt data and use two-factor authentication where possible.
10. If you use a wireless network, make sure that it is secure.
11. Monitor, log, and analyze successful and attempted intrusions to your systems and networks.

US-CERT.gov

The United States Computer Emergency Readiness Team (US-CERT) has numerous tips and resources on topics like choosing and protecting passwords, email attachments, and safely using social networks

FBI.gov

The Federal Bureau of Investigation leads the national effort to investigate high-tech crimes, including cyber-based terrorism, computer intrusions, online sexual exploitation, and major cyber-crimes.

CyberCrime.gov

Cybercrime.gov is the Department of Justice component responsible for implementing national strategies in combating computer and intellectual property crimes worldwide.

StaySafeOnline.org

The Stop.Think. Connect. ™ Campaign is a cooperative agreement between the Department of Homeland Security and the National Cyber Security Alliance (NCSA). Get more information about the Stop.Think. Connect. Messaging Convention, which is the formal way industry participates in the Campaign.

NIST.gov/CyberFramework

The National Institute of Standards and Technology developed the Framework for Improving Critical Infrastructure Cybersecurity. The Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure and help owners and operators of critical infrastructure manage cybersecurity-related risk.

Critical Infrastructure Cyber Community C³ Voluntary Program

The Critical Infrastructure Cyber Community C³ Voluntary Program is the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes through the use of the Framework.

URL = https://www.dhs.gov/sites/default/files/publications/Small-Business-Tip-Card.pdf

Cyber Crime Poses Threat to Autonomous Shipping, December 14, 2016, Alex Lennane

(The Loadstar) – Cyber-crime is likely to delay the introduction of autonomous ships for several years – and it could pose a significant threat to the shipping industry if it fails to act soon. There has been much progress on autonomous ships this year, notably from Rolls-Royce, and in October Norway opened the world's first designated test area. But there is still a long way to go, believes SeaIntelligence CEO Lars Jensen.

"Autonomous ships are a long way in the future," he told delegates at TOC Middle East in Dubai last week.

"They have to be built to better specifications than current ships. Who will repair them?

"They need to be more resilient. And what is the cost? What will we save from it? That has to be worked out."

One of the biggest problems facing the industry – and autonomous ships – is that it is not yet fully equipped to handle cyber- crime, he added.

"The industry is in very poor shape when it comes to cyber security. It needs awareness among senior management – this is not an IT issue.

"Firewalls and anti-virus software will not keep out dedicated attacks. If you think you haven't been hacked – you are wrong."

Mr. Jensen also warned ports and terminals that they were likely to be in the vanguard of cyber-attacks.

Noting several attacks in the past few weeks alone; that took out major sites such as Netflix and Twitter, as well as a telecoms company in Libya and another on domestic routers in Germany, he emphasized the vulnerability of ports, particularly via the Internet of Things.

"When you start to think of hardware in ports and terminals, everything has to be secure. We can put a lot of things online – but should we? There are thousands of gadgets in a terminal, and if they are online, they will be attacked."

Mr. Jensen set out the groups which would be most likely to attack – although he pointed out that staff could be a company's biggest concern.

"Staff are the worst – but often through negligence or incompetence. The most successful attacks compromise a person. It could be a disgruntled employee, or a trick which makes them reveal details."

But this could be mitigated by training, he said. While criminals are "plentiful and very good at cyber-crime", Mr. Jensen thought the biggest risks to the shipping industry were states, or state-sponsored groups – not necessarily terrorists.

"Ships and ports are clearly state infrastructure."

He said shutting down a major port in a hostile state would certainly be in the interests of some governments.

The good news, however, is that cyber-crime can be combatted without huge investment, he believes.

Companies should be looking to prevent crime at the design stage of technology – and simply encryption, understanding the risk and training would be critical.

"Companies need to work cyber defense into their business processes," he advised.

"Don't automate any deals worth more than $1m, for example. Improve staff awareness and technical know-how. It's not expensive – companies already have most of the tools they need. It's about training and configuring networks slightly differently."

The Loadstar is fast becoming known at the highest levels of logistics and supply chain management as one of the best sources of influential analysis and commentary.

Check them out at TheLoadstar.co.uk, or find them on Facebook and Twitter.

IMPORTANT NOTIFICATION CONTACT INFORMATION

Companies, facilities or vessels required to have a Marine Transportation Security Act (MTSA) security plan must report cyber intrusions and every other security breach to the Coast Guard's National Response Center (NRC):

- Phone 1-800-424-8802 or direct phone line at 202-372-2428
- Fax 202-372-2920
- Web: http://www.nrc.uscg.mil/

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
- IngraGard 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 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.