NORTHERN CALIFORNIA
AREA MARITIME SECURITY COMMITTEE
CYBER SECURITY NEWS LETTER
October 2017 (edition 2017-4)

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

- **NVIC 05-17 (Draft) –** a summary of the U.S. Coast Guard’s DRAFT Navigation and Vessel Inspection Circular 05-17 for cyber security measures.
- **Cyber Threats Prompt Return of Radio for Ship Navigation Threats Prompt Return of Radio for Ship Navigation –** an article about the world-wide impetus to implement a GPS back-up system in the form of eLoran.
- **Three Ways to Protect Your Supply Chain from Cyber-Attack –** an article about common sense cyber security considerations.
- **Maritime Cyber Security: Good, Better & Best –** discusses cyber-security as an industry necessity with available generic options.
- **The Promise and Peril of Smart Devices –** discusses the pitfalls of the use of modern smart devices, especially their susceptibility to misuse and hacking.

MAIN ARTICLES

NVIC 05-17 (Draft), USCG, Mr. Paul Martin, September 8, 2017

The long awaited (draft) Navigation and Vessel Inspection Circular 05-17 (NVIC 05-17) was published in the federal register in mid-July 2017 for public comment; the comment period ended on October 11, 2017. At 37 pages, it is too lengthy to include in this newsletter, however this article presents some of its highlights.

The NVIC's purpose is to have MTSA-regulated facilities analyze their vulnerabilities with computer systems and networks as part of their Facility Security Assessment (FSA). NVIC 05-17 will assist Facility Security Officers (FSOs) in completing this requirement. Additionally, NVIC 05-17 provides guidance and recommended practices for Maritime Transportation Security Act (MTSA) regulated facilities to address cyber related vulnerabilities. Until specific cyber risk management regulations are promulgated, facility operators **may use NVIC 05-17 as guidance** to develop and implement measures and activities for effective self-governance of cyber vulnerabilities.

NVIC 05-17 provides two enclosures to help port stakeholders in conducting their cyber risk assessment:

- **Enclosure (1)** provides draft interpretive guidance regarding existing regulatory requirements in 33 CFR parts 105 and 106, which instruct facilities to conduct FSAs and address any vulnerabilities identified in the FSA in the Facility Security Plan (FSP). This guidance details how those existing requirements relate to cybersecurity measures, and what is recommended to be included in the FSP.

- **Enclosure (2)** provides draft guidance to implement a cyber risk management governance program to include establishment of a cyber risk management team, policies, programs, and identification of critical systems. This guidance is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and NIST Special Publication 800-82, and provides more detail regarding the development of a Cyber Risk Management Program (CRMP) and specific examples as to how such a program can be implemented in a variety of system and business configurations.

The Maritime Transportation Security Act (MTSA) regulations are designed to provide the general parameters for port and facility security while allowing facility owners and operators the discretion to determine the details of how they will comply. The result is that the owners and operators are responsible for assessing vulnerabilities and ensuring the security of their facilities with Coast Guard oversight and guidance. The Coast Guard currently has the regulatory authority to instruct facilities and Outer Continental Shelf (OCS) facilities regulated under

MTSA to analyze computer systems and networks for potential vulnerabilities within their required FSA and, if necessary their FSP.

The maritime industry continues to increase use of cyber technology. Facility operators use computers and cyber dependent technologies for communications, engineering, cargo control, environmental control, access control, passenger and cargo screening, and many other purposes. Facility safety and security systems, such as security monitoring, fire detection, and general alarm installations increasingly rely on computers and networks.

Collectively these technologies enable the Marine Transportation System (MTS) to operate with an impressive record of efficiency and reliability. While these computer and network systems create benefits, they are inherently vulnerable and could introduce new vulnerabilities that increase the potential for risk. Exploitation, misuse, or simple failure of cyber systems can cause injury or death, harm the marine environment, disrupt vital trade activity, and degrade the ability to respond to other emergencies.

There are many resources, technical standards, and recommended practices available to the marine industry that can help their governance of cyber risks. Facility operators should use those resources to promote a culture of effective and proactive cyber risk management.

A copy of the DRAFT Navigation and Vessel Inspection Circular 05-17 (NVIC 05-17) is posted in the COTP San Francisco Zone section of the USCG HOMEPORT website at:

https://HOMEPORT.uscg.mil.

Cyber Threats Prompt Return of Radio for Ship Navigation Threats Prompt Return of Radio for Ship Navigation, Reuters, Jonathan Saul, August 7, 2017

The risk of cyber-attacks targeting ships' satellite navigation is pushing nations to delve back through history and develop back-up systems with roots in World War Two radio technology. Ships use GPS (Global Positioning System) and other similar devices that rely on sending and receiving satellite signals, which many experts say are vulnerable to jamming by hackers. About 90 percent of world trade is transported by sea and the stakes are high in increasingly crowded shipping lanes. Unlike aircraft, ships lack a back-up navigation system and if their GPS ceases to function, they risk running aground or colliding with other vessels. South Korea is developing an alternative system using an earth-based navigation technology known as eLoran, while the United States is planning to follow suit. Britain and Russia have also explored adopting versions of the technology, which works on radio signals.

The drive follows a series of disruptions to shipping navigation systems in recent months and years. It was not clear if they involved deliberate attacks; navigation specialists say solar weather effects can also lead to satellite signal loss. Last year, South Korea said hundreds of fishing vessels had returned early to port after their GPS signals were jammed by hackers from North Korea, which denied responsibility. In June this year, a ship in the Black Sea reported to the U.S. Coast Guard Navigation Center that its GPS system had been disrupted and that over 20 ships in the same area had been similarly affected.

U.S. Coast Guard officials also said interference with ships' GPS disrupted operations at a port for several hours in 2014 and at another terminal in 2015. It did not name the ports. A cyber-attack that hit A.P. Moller-Maersk's IT systems in June 2017 and made global headlines did not involve navigation but underscored the threat hackers pose to the technology dependent and inter-connected shipping industry. It disrupted port operations across the world.

The eLoran push is being led by governments who see it as a means of protecting their national security. Significant investments would be needed to build a network of transmitter stations to give signal coverage, or to upgrade existing ones dating back decades when radio navigation was standard. U.S. engineer Brad Parkinson, known as the "father of GPS" and its chief developer, is among those who have supported the deployment of eLoran as a back-up. "ELoran is only two-dimensional, regional, and not as accurate, but it offers a powerful signal at an entirely different frequency," Parkinson told Reuters. "It is a deterrent to deliberate jamming or spoofing (giving wrong positions), since such hostile activities can be rendered ineffective," said Parkinson, a retired U.S. Air Force colonel.

KOREAN STATIONS

Cyber specialists say the problem with GPS and other Global Navigation Satellite Systems (GNSS) is their weak signals, which are transmitted from 12,500 miles above the Earth and can be disrupted with cheap jamming devices that are widely available.

Developers of eLoran – the descendant of the loran (long-range navigation) system created during World War II – say it is difficult to jam as the average signal is an estimated 1.3 million times stronger than a GPS signal.

To do so would require a powerful transmitter, large antenna and lots of power, which would be easy to detect, they add.

Shipping and security officials say the cyber threat has grown steadily over the past decade as vessels have switched increasingly to satellite systems and paper charts have largely disappeared due to a loss of traditional skills among seafarers. "My own view, and it is only my view, is we are too dependent on GNSS/GPS position fixing systems," said Grant Laversuch, head of safety management at P&O Ferries. "Good navigation is about cross-checking navigation systems, and what better way than having two independent electronic systems."

Lee Byeong-gon, an official at South Korea’s Ministry of Oceans and Fisheries, said the government was working on establishing three sites for eLoran test operations by 2019 with further ones to follow after that.

But he said South Korea was contending with concerns from local residents at Gangwha Island, off the west coast. “The government needs to secure a 40,000 pyeong (132,200 square-meter) site for a transmitting station, but the residents on the island are strongly opposed to having the 122 to 137-meter high antenna,” Lee told Reuters.

In July, the United States House of Representatives passed a bill which included provisions for the U.S. Secretary of Transportation to establish an eLoran system. “This bill will now go over to the Senate and we hope it will be written into law,” said Dana Goward, president of the U.S. non-profit Resilient Navigation and Timing Foundation, which supports the deployment of eLoran. “We don’t see any problems with the President (Donald Trump) signing off on this provision.” The previous administrations of Presidents George W. Bush and Barack Obama both pledged to establish eLoran but never followed through. However, this time there is more momentum.

In May, U.S. Director of National Intelligence Daniel Coats told a Senate committee the global threat of electronic warfare attacks against space systems would rise in coming years.

“Development will very likely focus on jamming capabilities against … Global Navigation Satellite Systems (GNSS), such as the U.S. Global Positioning System (GPS),” he said.

In May, U.S. Director of National Intelligence Daniel Coats told a Senate committee the global threat of electronic warfare attacks against space systems would rise in coming years.
“Development will very likely focus on jamming capabilities against … Global Navigation Satellite Systems (GNSS), such as the U.S. Global Positioning System (GPS),” he said.

SPOOFING DANGERS

Russia has looked to establish a version of eLoran called eChayka, aimed at the Arctic region as sea lanes open up there, but the project has stalled for now. “It is obvious that we need such a system,” said Vasily Redkozubov, deputy director general of Russia’s Internavigation Research and Technical Centre. “But there are other challenges apart from eChayka, and (Russia has) not so many financial opportunities at the moment.”

Cost is a big issue for many countries. Some European officials also say their own satellite system Galileo is more resistant to jamming than other receivers.

But many navigation technology experts say the system is hackable. “Galileo can help, particularly with spoofing, but it is also a very weak signal at similar frequencies,” said Parkinson.

The reluctance of many countries to commit to a back-up means there is little chance of unified radio coverage globally for many years at least, and instead disparate areas of cover including across some national territories and shared waterways. The General Lighthouse Authorities of the UK and Ireland had conducted trials of eLoran but the initiative was pulled after failing to garner interest from European countries whose transmitters were needed to create a signal network. France, Denmark, Norway and Germany have all decided to turn off or dismantle their old radio transmitter stations. Britain is maintaining a single eLoran transmitter in northern England. Taviga, a British-U.S. company, is looking to commercially operate an eLoran network, which would provide positioning, navigation and timing (PNT). "There would need to be at least one other transmitter probably on the UK mainland for a timing service," said co-founder Charles Curry, adding that the firm would need the British government to commit to using the technology. Andy Proctor, innovation lead for satellite navigation and PNT with Innovate UK, the government's innovation agency, said: "We would consider supporting a commercially run and operated service, which we may or may not buy into as a customer."

Three Ways to Protect Your Supply Chain from Cyber-Attack, The Maritime Executive, Rick Williams, August 29, 2017

Threats on cyber-security serve as wake-up calls to businesses across industries. When threats or attacks hit close to home, like the recent cyber-attack on Maersk Line, you might feel a heightened sense of urgency to review your own contingency plan. While any supply chain has the potential to become a target, there are steps you can take to protect your maritime supply chain. By analyzing cyber-risks in advance, you can prepare to defend against them instead of waiting until after you've been attacked.

Ocean supply chains are subject to both regular market disruptors and potential future disruptors, and both can impact your supply chain. Regular events, like traditional peak season in North America from August to October, make it more challenging to obtain space on ocean vessels. But because these events occur like clockwork, you can take proactive steps to lessen their impact on your supply chain. For example, you can look ahead at your three-month forecasts and book the space you will need at least 2 to 3 weeks before you need it.

Cyber-attacks fall into the category of potential future disruptors. Like the regular disruptors, they can force you to use expedited shipping methods to meet delivery times. And because you may not know how long the disruption will last, the impact on your budget can be significant.

Ocean supply chains are particularly vulnerable to cyber-attacks, because your company is connected with parties in other countries with varying degrees of security measures. You will need to identify where your supply chain may be vulnerable. Then, work with your suppliers and ocean freight providers to develop scenarios for how you can recover from a variety of threats. ***The first step in this process is to think wider and deeper to understand your true risk exposure. Here are a few ways you can do that.***

1. Take a closer look at your electronic relationships.

We live in an interconnected world. Your business is not only connected with first tier suppliers and ocean providers, but with all of their electronic business partners. So, examine the electronic relationships you have with your ocean providers and suppliers. But don’t stop there; examine the relationships beyond your immediate partners.

For example, maybe you’re confident that your data is safe and sound with your first-tier connections. However, their electronic connections to other suppliers may not be as secure, and these second-tier suppliers can impact your cyber-security.
Start developing a complete supply chain network connection map that extends at least one tier beyond your direct customer/supplier relationships. Such a map can reveal unexpected dependencies and vulnerabilities and enable you to plan with your business partners to mitigate potential risks.

2. Prioritize the threats you deem most viable.

Take the obvious steps that are recognized as effective deterrents, like making sure you apply regular software updates and patches and offering basic security education to all employees. Then, go one step further.
Rank the threats to the technology and data assets in your maritime supply chain—computer equipment, mobile phones and tablets, and employee, customer, and financial data. Address the highest-risk areas first with the greatest scrutiny and urgency.

3. Host a cross-functional discussion within your organization to debate and implement recovery methods.

It’s important to understand how your organization identifies and mitigates other risks in the business. Then, align your ocean planning against cyber-attacks with the organization’s overall attitude toward risk and its expected time to recover. Your ocean cyber-attack planning will not be one-and-done. You will need to revisit and update the strategy continually, and test recovery methods regularly to ensure they remain relevant and can achieve your expected time to recover. Often, the organizational discussion that ensues among your leadership team and the extended discussion that occurs with your business partners can result in even more best-practice sharing.

Final thoughts

What all this teaches us is that disruptions from cyber-attacks can happen to any of us and for the ocean providers and suppliers we work with. It’s critical we all work together to prepare our supply chains if we want to prevent disruption for customers. Maritime supply chain disruptions can be unavoidable, but there are ways to prepare for events that may hold up shipping processes. Make sure your ocean shipping strategies are optimal.

Maritime Cyber Security: Good, Better & Best, Maritime Reporter & Engineering News, Rolf Berge, May 2017

[Editor's Note: The United States Coast Guard does not endorse or support the use of any specific cybersecurity product. The product discussed by the author of this article, serves only an example of cybersecurity software solutions and capabilities.]

As an industry that spends a great amount of its resources procuring and sending data in order to operate, the maritime industry is an attractive target for cyber criminals. Due to the remote locations of vessels and limited staff aboard ships and rigs, organizations and their offshore vessels and platforms are often ill equipped to ward off cyber threats. The cost and repercussions of a breach can be extensive in terms of both money and crew safety. According to a recent study, the cost of cybercrime has even surpassed that of drug crime. While cyber breaches are on the rise, they can be prevented with the proper preparation.

Be Prepared

Being prepared is the first step in securing your data against cybercrime. This includes ensuring all individuals within a company understand the importance of security, from top-level management to base-level employees. Top leadership needs to set an example and focus on requiring network safe guards while raising awareness of the importance of keeping systems and data secure. If management isn't concerned about it, then employees further down in the company will be relaxed about it as well and unconcerned about how they tend to the network. Cyber security should be on the agenda of the Company Board.

A lack of preparation can lead to dire consequences when the employees installing and maintaining network devices are too relaxed or unaware of potential threats to security. Often in these situations, network ports of these devices can inadvertently be left open, devices aren't properly configured, or software patches and updates are skipped, putting the company at risk. As 42 percent of cyber security risks are caused by careless insiders, proper training is essential to safeguarding a company's network.

When evaluating cyber security needs, a company should ask the following questions:

- What data would be considered most valuable to a cybercriminal?
- What training and safeguards are in place to minimize employee threats?
- Is there a cyber security solution already in place?
- If so, is there a formal way to evaluate the effectiveness of the security?
- Is there a disaster recovery plan if things go wrong?

Answering these questions will help a company determine next steps, whether that means implementing new security solutions or simply enhancing those already in place. While there are many different levels of security a company can implement to safeguard their data, the best solutions involve defense, monitoring and prevention. *Speedcast*, the critical communication company, is a great example of a firm providing such capability.

Proactive Solution

Speedcast's SafePass Pro combines the best of content filtering and monitoring with threat management services, including vulnerability assessments. With this combination of solutions, clients can benefit from working with *Speedcast* cyber security experts to pinpoint system vulnerabilities, monitor insider threats, proactively defend the network and respond to incidents. *SafePass Pro* is broken down into three different levels to defend, monitor and prevent cybercrime within the client's system. Altogether, this solution improves network resources, minimizes malware and spyware, enables centralized control across all sites, enforces acceptable use and security policies (AUP) and provides an opportunity to assess and eliminate network weaknesses. With that in mind, let's look at the good, better and best guidelines and options for protecting your system:

Level 1 - Defend - Good

This first, basic level is a firewall to keep unwanted visitors out. Most can filter traffic based on URLs, or classes of URLs, and single applications.
This can often be customized to customer needs or wants, with enhanced, granular blocking capacity to go deep into the types of classes of URLs to block - down to both geography and type of applications. With this level, the client can block users from accessing any site or application at risk for malware or other cyber threats.

Level 2 - Monitor - Better

The second level would build on the basic firewall defense mentioned in level one. This would be a monitoring service that reviews traffic that goes in and out of a client's network - whether that is a tanker, cruise ship, oil rig, semi sub or a single offshore vessel. All traffic is monitored by an appliance onsite that checks for any anomalies, strange traffic or patterns of traffic that suggests it is unwanted or could present a risk. At the discovery of such a threat, an alert is sent to the security operations center, for further action.

Level 3 - Prevent - Best

The third and final level is the preventative level. This level allows the customer to work with experienced firms like Speedcast on more of a consulting basis to perform vulnerability assessments. This is done by assessing open source threat intelligence to find out what information is present on the deep web or darknet that could represent a threat for the customer. This could be anything from financial data, key intellectual property or plans as well as entryways into on-board monitoring and control systems.

Chatrooms provide forums for bartering such information. Knowing that the information openly available on the internet is only 4 percent of the total Internet content and that the other 96 percent is hidden (i.e. deep web and darknet) , there is a vast amount of data that can be assessed to find out what types of threats the client is vulnerable to. Navigating this gargantuan amount of information in clandestine places in the darknet and identifying data representing threats requires skill and experience.

Additionally, this level of engagement provides more than simply finding out what is out there, but also provides the client with variations of penetration testing. This means that cyber security experts conduct tests to see how well a customer's security system protects their network. Even though a client may have blocked sites and is monitoring all the traffic going in or out of their network, there can still be vulnerabilities in the network itself through open ports or unpatched software on devices. This testing helps dive into any remaining problems to tighten security solutions.

Finally, clients have the opportunity to sit with companies such as Speedcast to review their current security stance including everything from how executives view the threat of cyber security and how they train employees, to the types of policies they have in place. This ensures proper training and threat management procedures can be implemented to safeguard from cyber threats.

Maritime companies without a cyber security solution leave themselves open to critical risks to their operation, and while having a program in place helps prevent these risks, an installation or network that isn't properly maintained or updated can be just as vulnerable. Taking proactive measures to ensure a company has a system in place that defends the network, monitors traffic and prevents cyber-attacks can provide peace of mind and prevent significant financial loss.

The Promise and Peril of Smart Devices, Stratford Board of Contributors, Jon Sather, August 23, 2017

In the world of espionage, developing and exploiting access to vital sources of information are the primary objectives. And these days, finding a way into information systems seems easier than ever amid the growing number of "smart" devices connected to our homes and businesses. Voice-controlled and hands-free microphones and speakers — Amazon's Echo and Alexa, Google's Home Assistant, Apple's Siri and Microsoft's Cortana, to name a few — welcome technology into our lives and trumpet the dawn of a new era: the age of artificial intelligence (AI) and the internet of things.

According to their makers, virtual home assistants are "always ready, connected and fast," "work across your devices, and integrate with hundreds of apps," and when you "tell it to do things … it's your own personal Google!" As these devices have proliferated exponentially and gained increasing acceptance, we have quickly adapted our lifestyles to their marvelous and intuitive technology. But take moment to consider the consequences: *Could somebody be using your devices to listen to and record your every move?*

Buyers Beware

A colleague recently purchased Alexa for his home and loves it. "Alexa is up and running, and it's slick. Seriously … for music it doesn't get any better." He has a point: Imagine the possibilities offered by a central device connected to many others, giving you the ability to monitor your home or control your appliances from afar.

"Alexa, start my car and set the air conditioner at 77 degrees. Alexa, play George Harrison's 'All Things Must Pass' album on my car's audio system. Alexa, remind me to stop at the grocery store after I leave work. Alexa, move all .xml work documents from my laptop to my office computer and file them under 'Finance.' Alexa, transfer $200 from my personal checking account to my wife's debit card." The last two commands may represent a stretch, but not by much. And if someone gains unauthorized access to your device, these fun and handy perks could quickly become nightmarish.

"Alexa, lock Master out of his car and send a ransom cell text for $800. Alexa, encrypt Master's MP3 music collection and send him an email saying 'get your music collection back for $20,000.' Alexa, turn Master's sprinkler system on every night from 02:00 to 05:00." There's no doubt that smart devices and the internet of things are useful. The technology they entail is well on its way toward creating an incredible amount of space and latitude in our everyday lives. But how carefully do we really consider how or if we make use of all its possibilities?

A Means to Many Ends

Smart technology carries some responsibility for manufacturers ("do no harm") and consumers ("caveat emptor") alike. And indeed, many producers — at least to some extent — put the protection of privacy and the security of information before their profit margins. *But an emphasis on caution in the use of smart devices rarely gets the amount of public attention it deserves*. After all, what company would drag down its own sales and turn away potential buyers by highlighting the vulnerabilities of its product?

Security experts have decried the internet of things as "ridiculously insecure." Just think of it: Baby monitors, light switches, security cameras, fire and smoke detectors, thermostats, and locks already are or can be made Wi-Fi ready. *Though that's great news for an individual customer, it's also great news for companies monitoring consumer spending patterns, for intelligence and law enforcement agencies, and for criminals.*

The weaknesses in the internet of things aren't just a problem for the ordinary citizen, either. Industries and businesses face the same risks, particularly as they move quickly to adapt to and profit from cutting-edge technology. During a recent business meeting at an unnamed high-tech company, a CEO asked: "Is the [industrial] internet of things really moving as fast as the marketers are telling us; that we'll soon have more connected machines than humans on Earth?" The question was quickly followed by a query of how best the firm could position its capabilities to leverage such rapid growth — a reasonable line of thought for a business hoping to keep up in an ever-changing world.

But for corporate security teams, there's another matter to consider. Centrally controlled and interconnected smart devices are pathways to industrial targets, whether information, proprietary secrets, business plans or employees' personal data. And they, too, are vulnerable to espionage by competitors, hackers and hostile state and non-state actors seeking to destroy, disrupt, steal, manipulate or delay data systems in order to achieve their own, at times nefarious, ends.

Tips for Taking Charge of Your Security

Governments haven't stood idly by as these threats have emerged. Washington, for instance, is considering the implementation of "baseline security protection." But it isn't yet clear whether this legislation will be shaped for simplicity or sophistication, for the lowest common denominator or for the most ideal outcome. Then there is the budding world of cyber insurance to consider: As a way to mitigate catastrophic risk, *cyber insurance seems increasingly popular and promising, but it is still untested and far from a fail-safe measure.*

Without a doubt, government regulation and cyber insurance are necessary components of a comprehensive IT security strategy, but they aren't sufficient — especially in an environment where security breaches linked to the internet of things are becoming the new norm. Instead, individual consumers and companies will have to take greater responsibility for their own protection by becoming better informed, personally invested and more motivated to invest in securing their devices.

To that end, it's important to stay aware of the access points that smart devices offer to would-be attackers. ***Below are 10 vulnerabilities to keep in mind:***

- ***Insecure web interfaces***: Many smart devices have built-in web servers that host web-based apps for managing the device. As is true of any web server or web-based app, there could be code flaws that render the device vulnerable to attack. Perpetrators can exploit these weaknesses remotely, and as an August InfoWorld report so aptly stated, users should "Assume the possibility of adversarial attacks on all in-production AI assets."
- **Ineffective authentication or authorization:** Though there are often weaknesses in authentication or authorization mechanisms themselves, the failure to make use of the features provided presents an even greater danger. *Convenience often trumps security when it*

comes to consumer behavior, and more often than not, individuals and companies will not take steps to fortify their defenses until they suffer a massive breach.

- ***Insecure network services:*** Smart devices may come with services for self-diagnostics, testing and debugging. But if they run on open, insecure or vulnerable ports, they, too, can rip holes in the devices' security. "Maintenance" services like these may be more likely to contain exploitable code, and though more features are often equated with a better device, it's important to remember that additional capabilities can come at a price.
- ***Lack of transport encryption:*** Most devices have encryption programs that operate seamlessly. But private information sent over an insecure protocol can be read by anyone. Connecting to a hotel room's Wi-Fi or always keeping Bluetooth on may allow an unintended party to access your information. *Users in search of additional encryption can investigate the option of using a virtual private network (VPN) or enhanced security apps created by companies like Norton.*
- ***Privacy concerns***: Many personal smart devices are configured to share information with friends, family and loved ones. But if the information in a device at rest is not encrypted, anyone who has access to it will have an opportunity to sift through personal data as well. *Therefore, it is important to know what information your smart device is sharing by staying aware of app, photo, social media and location auto-share settings.*
- ***Cloud connection:*** A sizable share of smart devices are connected to the cloud. If those devices feature a cloud management interface, they are more open to a remote attack than are management interfaces connected to the device's internal network. *That said, the latter are also less likely than cloud management interfaces to receive regular security patches*.
- ***Insecure mobile interfaces:*** Smart devices often feature mobile interfaces. But each new management interface serves as another breach waiting to happen. And because designing secure software is a complex and costly endeavor, it's not uncommon for producers to take shortcuts. Users should limit their exposure to a level they are comfortable with and update apps routinely. *(Updates nearly always include patches intended to improve device security.)*
- ***Insufficient security features:*** Even for consumers who are well-versed in the perils of personal technology, some smart devices have only limited security features to work with. For example, some products constrain the use of a PIN, while others may not allow the user to select an encryption option or access activity logs. To mitigate the ever-present threat of undetected data theft, research companies offering better, more secure services such as McAfee, Norton and PC Matic.
- ***Insecure software or firmware:*** Undetected flaws in software or firmware are often found after devices already have been released for sale. Some can be easily fixed with a patch, while others might require a complicated installation. Still others may destroy a device's ability to function. The same can be said of patches themselves: *Fraudulent "fixes" may, in fact, be designed to inject a malicious agent onto a device.* Consumers should install only original apps, software updates and patches created by the parent company (Amazon, Microsoft, Apple and Google, for example).

- ***Refurbished devices***: Smart devices that have been outpaced by newer models or abandoned by previous owners often make their way to eBay or Amazon. But if you are buying or selling a refurbished product, it is critical to ensure that the former owner's access information, data and commands have been wiped. Use caution and good sense, and if you outgrow a device and want to swap it for the latest features, consider destroying the old model and buying its replacement brand-new.

Smart devices have enormous potential to bring positive value to our lives. But they may also bring in the bad. So, buyers beware, make a routine of your own security and proceed with caution.

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.