#18

MAY: 2018

PHISH & SHIPS

BE CYBER AWARE AT SEA

Kindly sponsored by

JWC INTERNATIONAL

SMART4SEA TRAINING AND EDUCATION AWARD 2018
UNSUNG HERO OF INDUSTRY: HIGHLY COMMENDED, SAFETY AT SEA AWARDS 2017
BEST CYBER AWARENESS CAMPAIGN, INTERNATIONAL CYBER SECURITY AWARDS 2017

2018 Training Award SMART4SEA

Welcome to "Phish & Ships", the maritime cyber security newsletter, keeping you up to date with the shipping and offshore industry initiative, "Be Cyber Aware At Sea".

Inside issue 18, sponsored by JWC International, a leading global training, consulting and special projects group, providing services to commercial shipping, superyachts and ports around the world, we bring you more news about maritime cyber security, or the implications of the shipping industry's vulnerability.

These problems are not going to simply go away, there is much work to be done. A fact reiterated in the latest Crew Connectivity report, which we cover in this issue.

Also in this latest issue, we look at the spread of business email attacks, and look at some of the key guidance to emerge from both flag States and Classification Societies. As well as other features, and our continuing A-Z of Cyber Security.

See https://www.becyberawareatsea.com/ for more details and please support our campaign and don't forget to download our free resources, including our poster campaign.

CREW CONNECTIVITY FINDINGS

The latest Crew Connectivity report has been released and reveals data from a survey of nearly 6,000 active seafarers carried out by consultancy Futurenautics.

The report states that 47% of respondents said that they had sailed on a vessel that had been the target of a cyber attack. The data also revealed that only 15% of seafarers had received any form of cyber security training. Just as alarming only 33% of seafarers said the company they last worked for had a policy to regularly change passwords onboard and just 18% of those polled said the company they last worked for had a policy to change default equipment passwords onboard.

The survey also revealed just how connected ships are becoming. More seafarers than ever before have access to connectivity and communications. Seafarers who can now use the internet at sea has increased by 527,000 since the last survey in 2015, and those who can access it for free has increased by more than 200,000.

75% of seafarers said the level of connectivity provided onboard did influence which ship operator they worked for. 92% said it had a strong or very strong influence on who they worked for—a rise of 14%.

The view from the report is that while seafarers are a highly IT-literate workforce, they are seemingly being hampered by a lack of training, policies and leadership from industry stakeholders around cyber resilience and security.

The authors of the report state that if properly resourced then seafarers could be a formidable line of defence, but too few are being given the right tools to keep themselves and the wider maritime ecosystem safe.

The crew communications services most wanted by seafarers, and not currently provided, were free in-port WiFi, a global low cost roaming SIM card and a low cost satellite phone.

The report, sponsored by KVH and Intelsat, can be accessed for free at http://www.crewconnectivity.com/?product=2018-crew-connectivity-survey-report

REPORTING ON CYBER SUCCESS

MARITIME CYBER ALLIANCE
SUPPORTED BY AIRBUS

The pilot phase of the Maritime Cyber Alliance, a joint project between Airbus, CSO Alliance and the organisation's technology partner, Wididi, is already bearing fruit.

This month, as well as a number of reports of attempted email frauds and a man in the middle attack, we received our first anonymous, verified report from a vessel at sea. The vessel was forced to drop anchor when a malware infection disabled navigation systems, as they waited for outside help. The crew estimated the loss of time at around $40,000, highlighting the fact that cyber is effecting shipping at sea.

Recently, the Maritime Cyber Alliance joined the Digital Ship Maritime CIO Forum in Hamburg to update attendees on progress and discuss ongoing efforts to educate the shipping and port sectors about the cyber risks they face and how best to mitigate them. We have completed 35 workshops which have been well received and responding to the high interest and demand, a new series will be announced at a city near you shortly.

Continuing with new exciting updates, CSO Alliance is delighted to announce that we are a key partner to Templar Executives who have joined forces with Wärtsilä to launch an international Maritime Cyber Academy in Singapore, one of the countries taking a significant stance against cybercrime.

The Maritime Cyber Alliance will be an important resource tailored to support the Academy as part of this industry leading initiative. Initially, the courses will be available for delivery in both Singapore and London, providing a valuable suite of education tools for the maritime industry at a time when it is finally beginning to get to grips with information and cyber-security.

You can find more information here: https://www.templarexecs.com/templar-wartsila-singapore-cyber-

SINGAPORE LOOKS TO 24/7 CYBER SECURITY OPERATIONS

Another development in the Lion City, has seen the Maritime and Port Authority of Singapore (MPA) announce the establishment of a round-the-clock cybersecurity operations facility by the third quarter of this year.

The Maritime Cybersecurity Operation Centre will augment the agency's capabilities for early detection, monitoring, analysis and response to potential cyberattacks, MPA said in its press release, adding that more details on this initiative will be announced subsequently.

The protection of critical information infrastructures (CIIs) is one of the key areas the agency will focus on as sector lead for maritime cybersecurity, it added.

This comes after Singapore's Cybersecurity Bill was passed in February this year, which deals with CIIs in particular. The owners of CIIs have to comply with codes of practice and standards of performance, conduct cybersecurity audits and risk assessments and participate in cybersecurity exercises under the Bill.

UNDERSTANDING BEC

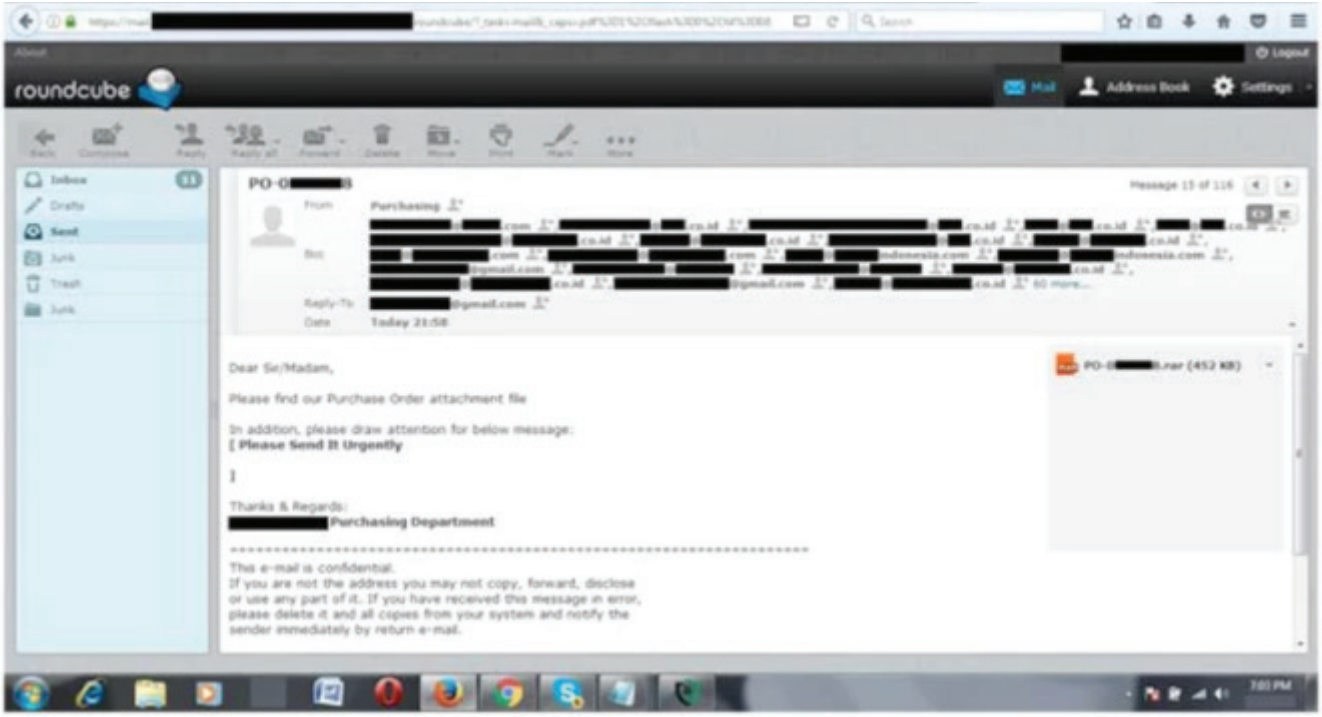
BUSINESS EMAIL COMPROMISE

A business email compromise (BEC) scam is a highly targeted attack designed to convince finance departments or C-suite executives to sign off on fraudulent invoices.

The attackers typically insert themselves in the middle of a legitimate business exchange using compromised email accounts, adding credibility to the attack, with the group in question even procuring a copy of a company's official invoice letterhead – by impersonating a client and asking for it.

NIGERIANS TARGET SHIPPING

NEW BREED OF NIGERIAN CYBER PIRATES AND THEIR SCAM EMAILS



A criminal gang in Nigeria has been running multiple "business email compromise" scams for hundreds of thousands of dollars. That alone would be bad enough, but they have also been targeting the global maritime industry.

According to security researchers, a group calling themselves, "GOLD GALLEON" have been sending messages to infiltrate payments within shipping and maritime companies.

The GOLD GALLEON group uses similar tools, tactics and procedures (TTPs) to other Business Email Compromise groups, typically using publicly available malware like inexpensive remote access trojans (RATs), crypters and email lures.

The group often targets smaller maritime companies, such as those who may provide ship management services, port services, and 'cash to master' facilities.

GOLD GALLEON appeared to identify target emails from looking at publicly available websites, and it also appeared to be using commercially available marketing tools to scrape email addresses – such as Email Extractor and BoxxerMail – as well as purchasing email address lists.

Once they gained access to a target's inbox, they extracted all the target's contacts – plus every email address that the target ever had an exchange with, using a free tool called EmailPicky.

After this initial recon, members targeted high-worth individuals with spearphishing campaigns, usually with a topic related to shipping. Attachments would deploy a RAT with keylogging capabilities. They used Predator Pain, PonyStealer, Agent Tesla, and Hawkeye – all available to buy online, with a basic version of Agent Tesla running for as little as $12.

Once they compromised an email, they would monitor inboxes for business transactions. They then inserted themselves into legitimate exchanges, submitting fraudulent invoices that would request payment to a mule account.

The gang would also buy domains that resembled the legitimate buyer or seller company name – lookalikes that would help them impersonate either party.

Victims have included a shipping company based in South Korea. GOLD GALLEON was able to steal credentials for eight accounts belonging to the company, including the accountant's. They then targeted all of the shipping company's clients.

The attackers monitored the business transaction of the South Korean company and a cash-to-master service for a ship arriving in America and inserted themselves into the transaction with a fake Outlook email account. They submitted a fraudulent email asking the South Korean company to deposit the payment into a "subsidiary bank account" – a mule operated by the criminals.

A separate attack saw GOLD GALLEON targeting another of this South Korean company's clients for $325,585, a large Japanese company that provides marine transportation of petroleum and chemicals with clients all over the world. The Japanese company, ultimately, had flagged the transaction as suspicious.

A third attempt against a separate multinational Japanese conglomerate for $243,838 was also derailed, with SecureWorks able to notify both parties and South Korean CERT – the incident response team in the country.

The researchers discovered that GOLD GALLEON appears to have a loose organisational structure, with the activities coordinated by a few senior individuals, who occasionally coached the junior members in what appeared to be mentoring roles, as well as liaising with other external criminal partners like suppliers of mule bank accounts.

They used proxy services to cloak their origin, but CTU said they had discovered evidence that many of their systems were regularly connecting to the internet via infrastructure based in Nigeria.

TOP10

ACT NOW TO CYBER SAFEGUARD YOUR FLEET....THE BASICS...

Pen Test Partners has been sharing their views on what you need to do TODAY to keep your fleet secure. Here is their Top Ten Tips:

#1 Make sure your satcom system isn't on the public internet: Most airtime providers offer a private IP address space, so hackers can't reach your satcom system as easily over the internet.

It's easy to find out if your vessel terminals are public or not: put the IP address in a browser and see if you can route to the terminal web interface from the public internet. Or you could port scan it. Speak to your airtime provider and check.

#2 Check that your satcom system has its passwords changed from the manufacturer default: By far the most common problem: the satellite terminal installer hasn't changed the admin passwords from the default admin/admin or similar. Ensure the passwords are complex and only known by those who need to know.

#3 Update the software on the satcom system: Make sure it's at the latest version and ensure it is updated every time the manufacturer publishes an update. Updates usually include fixes for security flaws, so the more out of date the software is, the more vulnerable it is.

Check the terminal vendors software update pages regularly – security fixes are often hidden in the changelog and not easy to find. This takes time and effort, so to spare the legwork consider using a patch update alerting service.

#4 Check that your bridge, engine room, crew, Wi-Fi and business networks on board are logically separated: If a device on your vessel is compromised, segregated networks will ensure critical systems are kept safe from the hacker. Do crew members personal laptops on the ship network have access to the navigation systems? Have you actually checked to make explicitly sure?

#5 Secure USB ports on all ships systems: It's very easy to accidentally get malware on USB keys. We've already seen cases of ECDIS and other systems compromised by ransomware. How often do you see a phone charging from a USB port on a bridge console? Phones can be full of malware too.

To prevent accidental introduction of malware to vessel systems, lock down USB access. If critical systems can only be updated by USB, keep dedicated USB keys in a secure location that are used for nothing other this purpose. This isn't ideal, but is better than open USB access!

#6 Check all on-board Wi-Fi networks: Strong encryption, strong Wi-Fi passwords and good Wi-Fi router admin passwords are a must. Crew Wi-Fi for personal use must not connect to anything other than the internet and/or on-board systems (e.g. media streaming) for personal use.

Any ship systems that use Wi-Fi (e.g. tablets for comms and navigation) MUST have raised security levels, including stronger authentication.

#7 Don't rely on technology: Officers of the watch must be reminded not to rely too heavily on technology and get fixated on screens. GPS can be spoofed, ECDIS position can be manipulated and even synthetic radar can be hacked to misreport.

Whether it's navigation, collision avoidance or using the "Mark 1 eyeball", each must be employed to ensure the situation outside the bridge reflects what the technology reports.

#8 Teach your crew about cyber security: Resources such as Be Cyber Aware At Sea are great for raising awareness and helping your crew avoid inadvertently opening the vessel to compromise.

#9 Make your technology suppliers prove to you that they are secure: If you don't ask for security, you don't get it! Your technology and services suppliers won't spend any time on security if they don't think the market wants it.

A 3rd party audit of your supplier would be a good start, though in the short term you should ask them for evidence of security accreditations such as ISO27001 or compliance with the NIST cyber security frameworks.

#10 get a simple vessel security audit carried out: Some of the worst vessel vulnerabilities are the easiest to find and fix. Bear in mind that maritime security issues are often systemic: they don't affect just one ship in your fleet, the same issue can affect them all.

See www.pentestpartners.com for the latest top tips...

A-Z OF CYBER SECURITY

F

G

H

I

J

F is for fileless threats. The success of a cyber attack largely depends on the likelihood of discovery, and attackers are using malware that never writes itself to the hard disk.

G is for Grayware, the divide between legitimate software and malware is often blurred. Grayware occupies the murky middle ground and may not have any recognisable malware concealed but can have troublesome files inserted.

H is for hacking, a catch-all phrase for all sorts of malicious activity from data breaches, to web page defacement, to bank fraud. Often it doesn't even involve any programming skill on the part of the attacker.

I is for Internet of Things (IoT) There was once a time when it was just computers that were connected to the internet. Then it was cellphones. Now, it's pretty much everything. Household appliances, security systems, heating and lighting, and even ships are now Internet-enabled.

J is for JavaScript, a widely used scripting language which is now the most popular file format for malicious email attachments. If you're lured into opening it, the script will run and download malware to your computer. Be warned..

source: medium.com

SAMSUNG WINS CLASS APPROVAL

Classification society ABS has granted a Certificate of CyberSafety Compliance for Samsung Heavy Industries' (SHI) Smart Ship Solution.

SHI's Smart Ship Solution is about improving vessel efficiencies using real time data from hull and equipment sensors in collaboration with land-based technical and fleet managers. Such real-time data transfer presents a growing cybersecurity challenge for the marine and offshore industries, ABS said.

According to the classification society, the shipbuilder's solution adheres to ABS Guide for Cybersecurity Implementation for the Marine and Offshore Industries and ISO 27000 series, IT Security Control Code of Practice.

ABS said it will work with SHI on next-generation cybersecurity technology for smart ships focused on both the ship's onboard architecture and its onshore fleet management cybersecurity architecture going forward.

DARING PORT CYBER RAID DISCUSSED

When people are searching for examples of what can happen when cyber criminals attack a port, one of the most often discussed is that of a daring scheme in the Belgian port of Antwerp. This has been the topic of recent debate once more. The attack saw criminals gain access to systems that controlled the movement of containers to smuggle cocaine, heroin and guns.

"It's a very sophisticated attack and they got away with it for a while before they got caught," says cybersecurity firm NCC Group's Andy Davis, who specialises in transport security. "These people look at the most effective approach that they can take to streamline whatever it is that they intend to do.

"They'll take advantage of the skillsets that are available to them. Although, yes, there have been demonstrations of things like spoofing GPS, spoofing automatic identification system (AIS) data, and taking ships off course – there are things like that you can do but they're technically much harder.

"If your goal is to steal cargo there are easier ways of approaching piracy than some of the more sophisticated headlines that have been demonstrated by security researchers."

CLASSIFICATION BODY MOVES FORWARD WITH CYBER GUIDELINES

IACS

International Association of Classification Societies

The International Association for Classification Societies (IACS) is aiming to deliver a set of guidelines covering cyber security practices in the shipping industry by the close of this year and present them to IMO.

The plan is to roll out 12 recommended practices that will make up an IACS risk framework on cyber resilience, and they are developing a risk model that can serve as a basis for managing cyber risk for vessels.

During the course of the year ahead, the body will also develop a parallel set of recommended practices that will help the industry address many of the challenges within the guidelines.

Importantly, the cyber guidelines will focus only on newbuild vessels. The reason for this, according to IACS secretary general Robert Ashdown, is to avoid duplicating the work of shipowning organisations.

"IACS is focusing on newbuilds because we're dovetailing that work with the operational guidance that is being developed by OCIMF and by BIMCO ... there's no point in us all working on the same things," he said. "IACS is working on the newbuild piece; that dovetails neatly with the operational piece developed by the shipowning organisations."

The organisation is attempting to ready shipping not for a far off vision of autonomous ships, but for the closer future when there will fewer officers attending to the machinery room, for instance. As far as IACS is concerned, then the cyber resilience of the vessel becomes extremely important.

See www.iacs.org.uk for more information.

EU CYBER SECURITY PROJECT DELIVERS ON AMBITIOUS MARITIME INDUSTRY GOALS

The EU research project MITIGATE has been completed and the ambitious goal of designing, developing and implementing a risk assessment and management system for the maritime transport chain in 30 months has been achieved.

At the beginning of the development many companies in the maritime transport industry stressed their need for support in assessing how well their IT assets (hardware and software components) are protected against attacks and how external and internal cyber attacks can be prevented.

The results of a survey among almost 200 maritime stakeholders showed that nearly two thirds of the companies responding did not carry out a risk assessment. They also expect a solution like MITIGATE to comply with national and international standards and regulations.

The result of the project work is a software environment that can be used cloudbased, but also locally in the company. It enables companies to map IT assets that support their business processes through data processing and data exchange. These assets are connected along an information chain and can be tested for known weak points and attack potentials. The information chain is connected virtually to the business partners without the assets used being disclosed to each other. Information about new vulnerabilities and threats is not only collected automatically from databases, but also from social networks and other Internet sources specializing in IT security.

Practical tests and evaluation of the software solution have involved more than 680 representatives of the maritime transport chain at more than 70 events. Test runs with real data and live demonstrations were used to adapt the system to the needs of users.

The vast majority assess the system positively and helpful for risk management. Information on the project and the status of commercial implementation can be found at www.mitigateproject.eu

REGISTER RELEASES GUIDELINES

The Marshall Islands has issued a Marine Guideline note (No.2-11-16) on Maritime Cyber Risk Management. The document identifies information sources that may aid in establishing policies and procedures for mitigating maritime cyber risks.

It also follows the IMO guidelines in setting out the following principlesin support of an effective cyber risk management strategy. As such, Marshall Islands vessels must be able to:

- **Identify:** Define the roles responsible for cyber risk management and identify the systems, assets, data and capabilities that, if disrupted, pose risks to ship operations.
- **Protect:** Implement risk control processes and measures, together with contingency planning to protect against a cyber incident and to ensure continuity of shipping operations.
- **Detect:** Develop and implement processes and defenses necessary to detect a cyber incident in a timely manner.
- **Respond:** Develop and implement activities and plans to provide resilience and to restore the systems necessary for shipping operations or services which have been halted due to a cyber incident.
- **Recover:** Identify how to back-up and restore the cyber systems necessary for shipping operations which have been affected by a cyber incident.

The full Guideline note can be found at:

https://www.register-iri.com/forms/upload/MG-2-11-16.pdf

CYBER NEWS IN SHORT

NOT ALL DOOM AND GLOOM

Lars Jensen, CEO and Partner at SeaIntelligence Consulting, has been speaking about the technological boom in the maritime industry, and the sector's reaction to new innovations and cyber security.

Jensen is one of the leading lights of maritime cyber security, and he believes that part of the problem is that shipowners are "bombarded with new technologies every day, but only some will be tested and trialled on board."

He states that increased connectivity and more digital activity bring the potential of cyber risks to any organisation. As such cybersecurity is definitely something the industry has to take a lot more seriously than it has done in recent years. a lot of what needs to be done is not rocket science. A lot of this is down to sheer awareness, it is down to keeping things updated. It is down to making things more secure.

Thankfully it is not all doom and gloom. According to Jensen, there is a lot that can be done on cybersecurity without necessarily having to spend tens of millions of dollars on advanced solutions.

Access the full interview here: https://bit.ly/2Ftosm5

QCs ON COMPENSATION

Will we soon see claims for compensation resulting from cyber-attacks in the maritime sector? Despite efforts to counter such attacks, it can only be a matter of time before cyber risks translate into actual claims against, and perhaps liability on the part of shipowners.

In a 20 Essex Street Bulletin, Karen Maxwell discusses this relatively new, and rapidly developing issue faced by owners which appears to have no harmonised standards and no clearly established "best practice".
Access the paper at: https://bit.ly/2jk9GWn

INSURER FEARS VOICED

Shipping industry firms and port operators are worried about linkage between cyber-attacks and supply chain risk, insurer XL Catlin has warned.

Big interdependencies between systems mean maritime firms face major business continuity risks from online threats.

"The problem is that nobody knows, other than the computer systems, where your goods are," said Pascal Matthey, head of global lines for marine risk engineering at XL Catlin.

"You might never find your container again. Refrigerated containers might lose power, which would mean huge damage," said Matthey.

He warned about the potentially catastrophic consequences of a cyber-attack by terrorists, such as targeting a ship and interfering with its steering or navigation to cause a collision in congested waters, such as a port or major trade artery such as the Panama Canal.

SINGAPORE EMERGES AS A LEADER IN CYBER SECURITY... AND CONFERENCES



Gideon Lenkey, Technology Director at EPSCO-Ra has seen the future of maritime cyber security events...here he shares his thoughts.

No matter what you do in Maritime, the subject of Cyber Security has probably been mentioned if you've attended a conference in the past year or two.

There are even Maritime industry conferences completely dedicated to the subject of Cyber Security. Having attended more conferences than I can immediately recall over the past two years, at least without pulling up receipts, boarding passes or counting conference lanyards, I can honestly say I've just attended perhaps the best one to date.

I was recently invited by the Singapore Shipping Association to be a panelist and presenter at their second annual Maritime Cyber Security Seminar as part of Singapore Maritime Week. I came away sincerely impressed by the mature and cohesive message being delivered to the attendees by the guests, panelists and presenters.

During this event the Maritime and Port Authority of Singapore (MPA) outlined their new Maritime Cyber Security Operations Centre, scheduled to roll out in the fourth quarter of this year.

This marks an industry first, since rather than being aimed at awareness or training, this will be a functional Security Operations Centre. The 24/7 SOC will have detection, monitoring, analysis and response capabilities entirely focused on Maritime incidents.

It's quite clear that Singapore takes the cyber security threat seriously and is willing to stake a leadership position by addressing it.

Throughout the entire conference there was a cohesive message that Cyber Security must be dealt with as a business process at the C-suite level and not just pushed onto IT for a technical solution. There were presentations which covered multiple data sets and offered expert analysis, conclusions and suggestions.

This was refreshing to hear at a Maritime conference, as more often than not the message you hear isn't one of analysis and useful advice but rather 'my company has just launched our great new product and it's really great, you should buy it'.

Now to be fair, and in the spirit of full disclosure, I work for a managed security services company but I don't think it's appropriate for vendors to buy their way onto the lectern to sell you a product when you've paid to be in the room. There were vendors at this conference.

However, they were invited and presented data analysis, case studies and advice, rather than direct sales pitches. I can see why this conference quickly sold out and I suspect it will again next year.

If you are considering attending a conference or seminar in the near future and you want to get the best experience for your money, here is some advice. Find events where the presenters are either invited or compete to present through a pre-event call for papers process. All the best cyber security industry hacker conferences do this, DefCon, ShmooCon, Derby Con etc.

You'll likely have a better experience than you will at events where the presenters simply sign up and pay to speak. You may have to call and ask or research online reviews to find this out as it's generally not mentioned in the promotional materials. That's not to say the content at pay-to-speak conferences is all bad. I've seen some valuable and even entertaining presentations at pay-to- speak conferences.

Unfortunately, I've also seen multiple, almost identical sales pitches back to back, which almost cleared the room. If you are reading this and are an event organizer in the Maritime conference or trade show industry, here is some advice. If your intention is to give your attendees the very best, keep them in their seats until the end of the day and bring them back to subsequent events, then you have to attract the best and brightest speakers and deliver useful, actionable content.

1 Hour MCA Recognised & GCHQ Approved Training

Maritime Cyber Security Awareness Course (MCSA)

The ‘human factor’ is your biggest vulnerability to cyber crime.

Educate your workforce today to protect themselves and your organisation tomorrow.

- Easy access 1-hour online course
- Designed to complement current approaches to cyber security
- Suitable for all personnel – onboard and ashore
- MCA Recognised and GCHQ Approved

JWC INTERNATIONAL

For more information or to book, please visit us: www.maritimecybertraining.online