Lloyd's List

# Cyber security

A special report

Lloyd's List

# Curated maritime news and market analysis

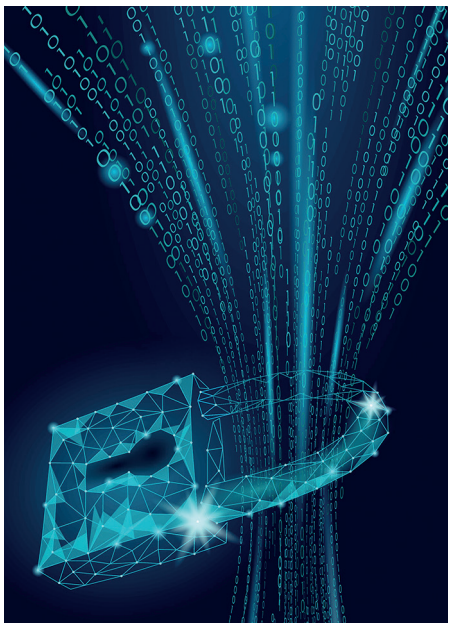
- Unrivalled news coverage
- 115k+ articles in our archive
- Correspondents in seven maritime hubs

## Choose the trusted source

Contact us today on **+44 20 7017 5392 (EMEA)** / **+65 6508 2428 (APAC)** / **+1(212) 502 2703 (US)** or visit **lloydslist.com**

# Cyber security

Cyber security has been put towards the top of shipping's risk list following a spate of high-profile attacks in recent years. Yet the industry's cyber resilience is still flattering to deceive. A Lloyd's List survey to examine the true extent of cyber attacks across the maritime sector and the measures being taken to deal with this growing threat led to some damning conclusions. Shipping's slow progress in addressing this online menace continues to play into the hands of cyber criminals.



LuckyStep48/Alamy Stock Vector




**Editor**
Linton Nightingale

**Lloyd's List Managing Editor**
Richard Meade

**Contributors**
James Baker, Nidaa Bakhsh, Declan Bush, Xin Chen, Richard Clayton, Bridget Diakun, Nigel Lowry, David Osler, Janet Porter, Adam Sharpe, Cichen Shen, Eric Watkins, Michelle Wiese Bockmann, Fred Williams, Robert Willmington

**Marketing Services**
Daniel Eckersall:
**daniel.eckersall@informa.com**

To advertise please email:
**marketingservices@informa.com**

**Asia Pacific**
Rezal Ibrahim

**Americas**
Rory Proud

**Middle East**
Shofiul Chowdhury

**EMEA**
Deborah Fish, Adrian Skidmore

**Greece**
Janet Wood

**Classified**
Maxwell Harvey

**Advertising Production Manager**
Mark Leech

**Production Editor**
Felicity Monckton

**Printing**
Paragon Customer Communications

**Editorial**
Lloyd's List,
240 Blackfriars Road,
London SE1 8BF
Tel: +44 (0)20 7017 5000
Email: **editorial@lloydslist.com**

Published by Informa UK Ltd.




Lloyd's List is available online in every country in the world by placing a subscription with the publishers in London, Informa UK Ltd.

Please place your order with the Lloyd's List marketing team at Informa. This special supplement is issued free to subscribers.

For further information please email:
**subscription.enquiry@lloydslist.com**
or telephone: +44 (0)20 3377 3792


Skorzewiak/Alamy Stock Photo

**Of those that participated in the survey, one in five said their companies had experienced a cyber attack in the past three years.**

# Shipping is falling short in cyber preparedness

Lloyd's List's survey raises concerns over shipping's cyber resilience, with the risk level of online threats only likely to increase, **Linton Nightingale** reports

The threat of cyber attack is high on shipping's risk list; however, a Lloyd's List survey has cast major doubt over whether the industry is doing enough to combat the online menace.

Lloyd's List polled its readers to reveal the true extent of cyber attacks across the maritime sector and how companies are dealing with this growing risk, providing some eye-catching results that will undoubtedly ring alarm bells.

Indeed, only one-quarter of the industry feels enough is being done to spread awareness, while just two-thirds have knowledge of measures in place if online systems are compromised.

The results serve as a wake-up call for shipping that while efforts have improved dramatically in recent years, the industry's cyber resilience is still falling short of the mark.

Shipping, like other industries, has seen numerous attacks on its businesses, causing major operational disruption and some significant financial losses.

At the time of writing, in the space of just one week, there were reports of a cyber attack at India's Jawaharlal Nehru Port, where operations at the port's state-run facility, the Jawaharlal Nehru Container Terminal, came to a standstill; while US logistics major Expeditors had also been hit by a further attack, forcing it to close its operating systems globally to limit the impact.

These add to an ever-growing list of shipping companies that have witnessed similar attacks, including shipbroking giant Clarksons, Chinese conglomerate Cosco and French container shipping line CMA CGM, to name just a few.

Even the International Maritime Organization has seen its systems compromised at the hands of online intruders.



# POWERING GLOBAL GATEWAYS

As a leading enabler of global trade, PSA has what it takes to drive change and realise sustainable growth. We innovate alongside our partners in the port and logistics industry to orchestrate greener trade and logistics. Partner with us to move the world's goods, for the greater good.

PSA

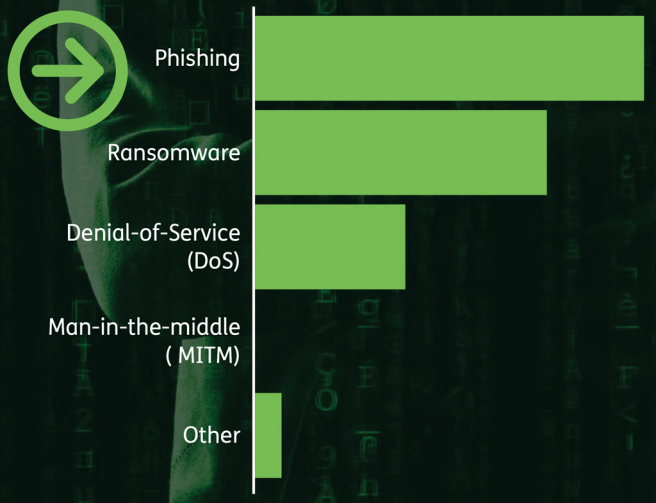
www.globalpsa.com

# Cyber-security survey

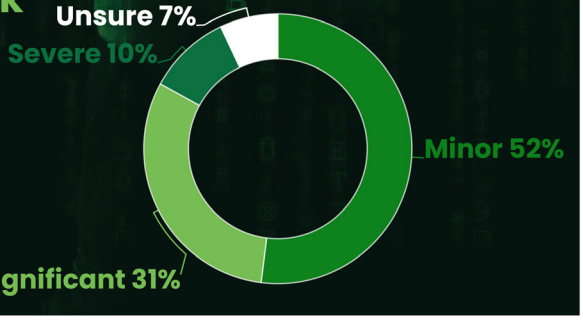
## Lloyd's List polled its readers to reveal the true extent of cyber attacks across the maritime sector and how companies are dealing with the growing risk

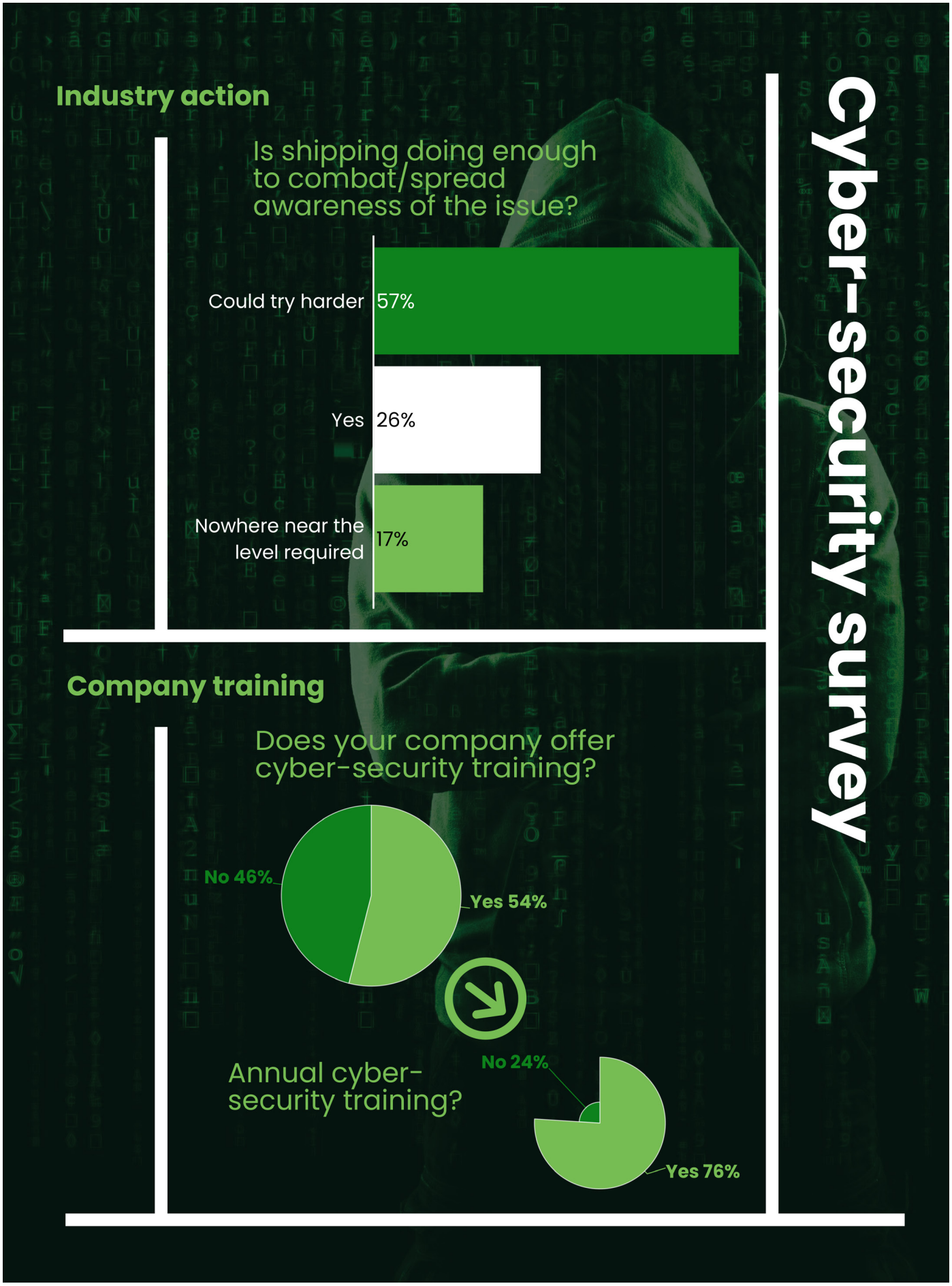
Has your company been the victim of a cyber attack in the past three years?

Yes No




### Severity of cyber attack

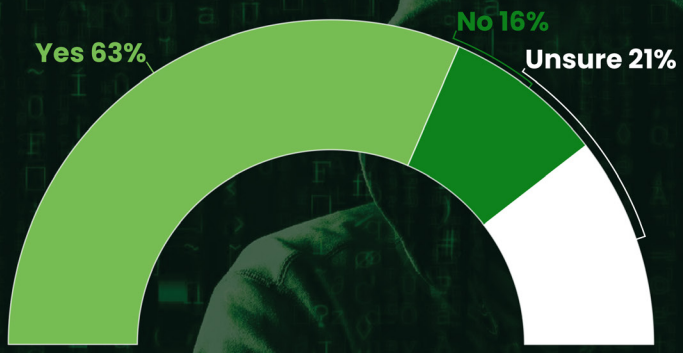



Cyber-security survey
Industry action
Is shipping doing enough to combat/spread awareness of the issue?
Could try harder 57%
Yes 26%
Nowhere near the level required 17%
Company training
Does your company offer cyber-security training?
No 46%
Yes 54%
Annual cyber-security training?
No 24%
Yes 76%

# Cyber-security survey

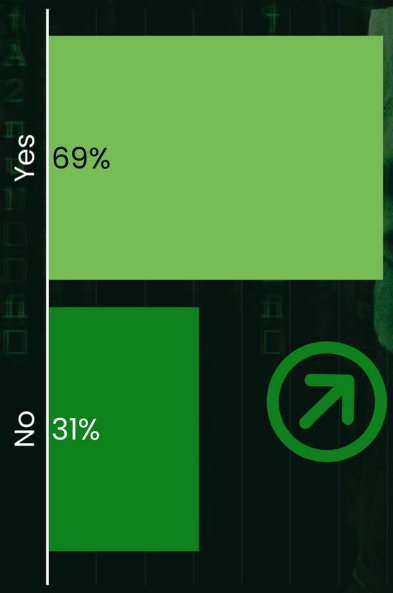
## Planning

Does your company have measures in place in the event of a cyber attack?




## Insurance provision

Satisfaction with insurance available




**Reasons for insurance dissatisfaction**

- *Administrative bottlenecks*
- *Failure to address true cost*
- *Varying levels of coverage*
- *Different company levels of concern and protection expectation*
- *High premiums*
- *Lack of policy clarity*
- *Limited availability*
- *No conduct standards*

GRIMALDI GROUP

# Worldwide Shipping and Logistics

MaritimeTransport and Logistics Solutions for any type of

**ROLLING CARGO • EARTH MOVING EQUIPMENT • STANDARD AND SPECIAL CONTAINERS**
**FORESTRY PRODUCT • PROJECT AND HEAVY LIFT CARGOS**


**ANTWERP**
Grimaldi Belgium
Tel: +32 3 5459430

**HAMBURG**
Grimaldi Germany
Tel: +49 40 789707 12

**LONDON**
Grimaldi Agency UK
Tel: +44 207 9305683

GRIMALDI GROUP
**www.grimaldi.napoli.it**

Yet arguably the most high-profile attack came in 2017, when AP Moller Maersk became an unintended victim of the NotPetya malware attack. The outage of Maersk's systems cost the group hundreds of millions of dollars and unwanted reputational damage.

If not for a power outage in Lagos, Nigeria, where systems were unaffected by the virus, ensuring back-ups could be retrieved, the situation could have been even worse.

Understandably, Maersk has since made cyber security a top priority, having learned the hard way, and is investing millions in online systems and personnel to mitigate further threats.

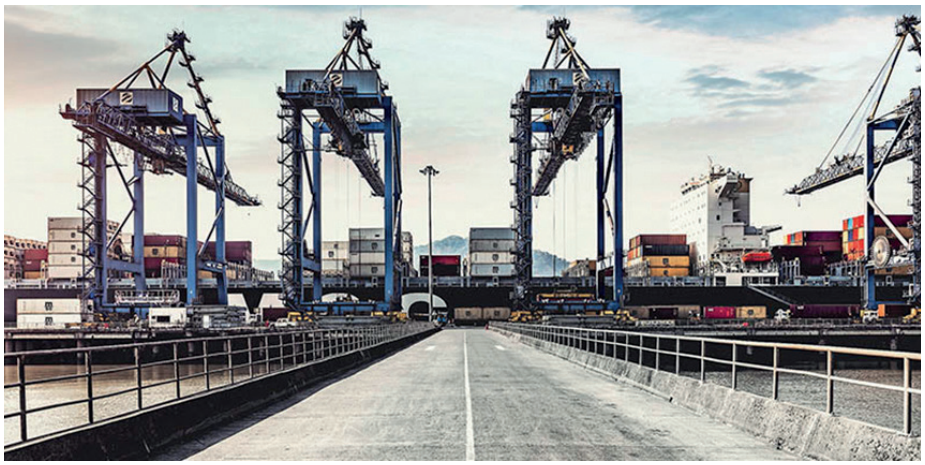
The industry has also made significant strides in creating awareness and guidelines for best practice.

Last year, the IMO introduced its first comprehensive cyber-security recommendations — and in the container shipping sector, for example, industry body the Digital Container Shipping Association published its cyber-security implementation guide back in 2020.

However, it is evident that efforts still leave much to be desired.

External commentators and cyber experts have suggested that another NotPetya-type attack, similar to the one that took down Maersk, may be required before shipping gives cyber security the attention it deserves.

The likelihood of such a scenario has only increased of late, amid concerns that Russia could use cyber warfare in retaliation to western sanctions enforced due to its invasion of Ukraine.



Jawaharlal Nehru Port Trust

**After a cyber attack at India's Jawaharlal Nehru Port, operations at the port's state-run facility, the Jawaharlal Nehru Container Terminal, came to a standstill.**

The fear is that shipping companies — and others — could inadvertently be caught in the cyber crossfire.

Further, the Global Maritime Issues Monitor 2021, a survey in partnership with the Global Maritime Forum and the International Union of Marine Insurance, ranked cyber attacks and data theft second for lack of preparedness on the critical issues facing maritime.

The results of Lloyd's List's cyber-security survey further underscores industry concern surrounding an issue that is not going away anytime soon.

With shipping increasingly relying on online applications to keep vessels and cargo moving, and to continue on its digitalisation path, the attack space for cyber crime and its actors is widening — and so too is industry vulnerability.

> *If we include everything, it is 100% [of companies that have experienced a cyber attack], but if you exclude some of the minor things, such as automatic emails from the 'Prince of Nigeria' as part of a phishing scam, then numbers will go down considerably*

**Lars Jensen**
Chief executive
Vespucci Maritime

## Room for improvement

The Lloyd's List survey drew responses from across the shipping industry. Shipowners (13%) were the most highly represented in the sample, followed by ship operators and shipmanagers (9%). Other organisations included those in the fields of financial services, consultancy, academia and logistics.

Of those that participated in the survey, one in five said their companies had experienced a cyber attack in the past three years, with phishing and ransomware being the most common forms of attack.

There were also examples of 'cross-site scripting', also known as XSS attacks, in which malicious code is injected into otherwise safe websites, and 'Denial-of-Service', when systems are effectively shut down, preventing users from accessing certain sites or programmes.

While the number of attacks is significant, Vespucci Maritime chief executive Lars Jensen told Lloyd's List that, in reality, this number could be 100%, as it would be difficult to find a single person that has not been subjected to a cyber attack in recent years.

This, he explained, highlights the issue of what constitutes a 'cyber attack', with a lack of a common vocabulary surrounding the subject.

"If we include everything, it is 100%, but if you exclude some of the minor things, such as automatic emails from the 'Prince of Nigeria' as part of a phishing scam, then numbers will go down considerably," said Mr Jensen.

Nevertheless, he also noted that while a regular employee would certainly notice a major cyber attack that impacts all systems, one that compromises a small portion of servers will only be acknowledged by the IT department.

There is also the issue that companies will often not report cyber attacks for fear of reputational damage — a factor not solely restricted to the shipping industry. This, too, would suggest that the number of attacks could be substantially higher than the level reported in our survey.

In terms of the severity of cyber attacks reported by survey respondents, around half of them only had a minor impact on operations, while two-fifths were seen to be more damaging to the organisation.

As stated earlier, one of the more alarming conclusions of the survey was how an overwhelming majority feel industry action leaves much to be desired.

Only one-quarter of respondents (26%) feel the shipping industry is doing enough to combat or spread awareness of the threat of cyber attacks, with as many as one-fifth stressing that "a lot more still needs to be done".

Bill Egerton, chief cyber officer at cyber insurer Astaara, said the majority of the larger shipping companies are taking appropriate action. They have capabilities in place to mitigate for attacks and are only too aware that you cannot "nickel and dime" when it comes to cyber security.

The concern, he said, lies with some of the smaller players: "There is a belief that they are too small to be noticed, which is a failure to appreciate that this is not size-dependent. If you're on the internet, you're a target."

CyberOwl chief executive of Daniel Ng felt that despite the obvious concerns, there has still been significant progress in cyber awareness, particularly over the past 18 months.

"We were having discussions back then as to why we even need to protect vessels, but the conversation has moved on. Now there is acceptance; now we're discussing how best to make smart decisions around protecting systems," he said.

"Can we do more? Absolutely. There is a lot of noise around maritime cyber security at the moment, and we need to take sensible steps to build up the sector and rise the tide, which requires smarter choices."

> *There is a belief [by smaller companies] that they are too small to be noticed, which is a failure to appreciate that this is not size-dependent. If you're on the internet, you're a target*

**Bill Egerton**
Chief cyber officer
Astaara

## Inadequate training

Of further concern was how just under half of all respondents said they were not offered cyber-security training — and only three-quarters of these had undertaken training in the past year.

Mr Egerton stressed that companies that are not training staff could be at risk of breaching the IMO's 2021 guidelines, resulting in regulatory sanctions — but also disproportionately large financial losses if hit.

"Training is a fundamental element of seaworthiness. When talking about safety of life and environmental protection on board vessels, if training is not undertaken in the cyber dimension, there is a serious issue. You cannot ignore the need to have people trained," he said.

Yet another damning reflection on the shipping industry was how one-third of those polled were either unaware of company processes or believe their company is not prepared for a cyber attack.

Mr Ng said this comes as little surprise, echoing his own experience on the ground. Although he said the industry has done a very good job in getting to the stage of putting IMO requirements in place, implementation is another thing.

"As a sector, we need to go further and get to a point where we're actually doing the things, we say we're doing. If we do, we'll have come a long way from a security standpoint," said Mr Ng.

Finally, the survey also garnered response on the level of satisfaction regarding cyber-liability insurance products offered by the industry.

Almost two-thirds of respondents noted they were happy with the products on offer. Those that were not satisfied, however, reiterated complaints familiar to cyber underwriters: that products on offer do not adequately cover the true cost of cyber attacks, including recovery and loss of business. And they are increasingly expensive, too.

Lorenzo Spoerry, deputy editor of Lloyd's List's sister publication, Insurance Day, noted how on current trends, market-wide cyber premiums are set to double every three years.

"The problem for underwriters is that, in contrast with other lines of business, cyber peril is ever-changing, making assessing the true scale of the threat uniquely difficult," he said.

"Some cyber specialists believe that cyber will be one of the most important lines of business within two decades. Yet many of the largest underwriters still take a very measured approach to providing coverage."


**The results of Lloyd's List's cyber-security survey will form part of the discussion in our upcoming webinar held in conjunction with our sister publication, Insurance Day, on March 20.**
**Details of how to register for the webinar, 'The cyber threat to maritime and the insurance industry's response', can be found via the Lloyd's List website.**


Denis Putilov/Alamy Stock Photo

**The most critical first step towards protection is for the C-suite to take responsibility for cyber risk.**

# Chief executives are first line in solid cyber-security defence

The human element is just as important as technology in beating the opportunists, hackers and state-backed cyber attackers, **Richard Clayton** reports

In its cyber-security guidelines for ports and port facilities, the International Association of Ports and Harbors (IAPH) describes cyber risk as the "unavoidable handmaiden" to digitalisation.

The number of cyber attacks on ports, shipping and the wider logistics supply chain cannot be accurately quantified. However, it is clear that the deeper the maritime industry gets into digitalisation, the more vulnerable it becomes.

Protecting the industry from hackers is not rocket science. Guidelines on cyber security have been issued from all the industry associations and are aligned with the International Maritime Organization's stipulation that cyber risks must be appropriately addressed in existing safety management systems no later than the first annual verification of the company's Document of Compliance after January 1, 2021.

The most critical first step towards protection is for the C-suite to take responsibility for cyber risk. Security is a collective remit that is not solely limited to the IT department.

"Senior management should embed a culture of cyber-risk management into all levels and departments of an organisation," states the latest version of industry guidelines led by BIMCO.

It adds that senior managers should ensure a "holistic and flexible" cyber-risk governance regime, which is in continuous operation and constantly evaluated through effective feedback mechanisms.

The significance of this first step is often overlooked in the rush for technical solutions.

"Being able to assure yourself, your clients and your supply chain of the integrity of the data flowing through and across your systems is becoming part of the fabric," Inmarsat Maritime president Ben Palmer told Lloyd's List.

"While it's an obvious truism, I'm not sure everyone has fully absorbed what it means in practice. Managing response plans and managing the reality of the situation will be 'de rigeur', as well as trying to ensure against it."

Mr Palmer, who brings experience to maritime from the defence and aviation sectors, said cyber security tends to be presented as a technological problem, although the human dimension is just as important.

> *"People tend to think about the standalone thing they own, but it's the interfaces where things go wrong. That makes it an enterprise problem as opposed to individual actors securing their bit of it"*
>
> **Ben Palmer**
> President
> Inmarsat Maritime

## Taking the lead

IAPH agrees. Its guidelines recommend that C-suite executives should take the lead in allocating resources to deal with cyber security, actively managing governance and building an organisational culture to support cyber-security operations, and developing leadership strategies for driving cyber resilience, including the creation of a cyber-security workforce.

The ports' association focuses on developing a business case for the executive team to determine a reasonable level of investment in cyber risk management. Its conclusion should be taken on board by ship operators and managers alike.

Port managers weigh up whether a proposed level of investment is enough and whether the return on investment justifies the spending.

They argue that trade-offs are constantly being made in a competitive world; that cyber risk is insurmountable — a belief that prohibits proactive investment in key resources; that cyber risk is difficult to quantify and depends on subjective analysis; and that the hardest thing to change is human behaviour.

Such justifications reveal a common perception plaguing executive suites: that investment in cyber security is often considered a cost centre, rather than an enabler of port operations.

Once the senior management is on board, the second step is to manage risk itself.

There are several elements to this, beginning by identifying the external and internal nature of threats, identifying which systems are liable to attack, and assessing exposure to risk.

Once vulnerability is understood, the necessary protections can be built. Protection and detection measures can be agreed, response plans established, and analysis made following a cyber incident.

gtzx/Alamy Stock Photo

**The ship-to-shore interface, where cyber security for ships and cyber security for ports overlap, can present one of the most vulnerable nodes of the supply chain network.**

The ship-to-shore interface, where cyber security for ships and cyber security for ports overlap, can present one of the most vulnerable nodes of the supply chain network.

"Think about the interfaces," Mr Palmer urges. "People tend to think about the standalone thing they own, but it's the interfaces where things go wrong, where there are leaks. That makes it an enterprise problem as opposed to individual actors securing their bit of it."

All cyber-security guidance stresses the importance of the human element alongside the technology. One document states: "It cannot be stressed enough how important it is to raise the awareness and vigilance of crews regarding cyber security.

"Crew training may look like a simple and inexpensive measure to implement, yet it represents the smartest investment in this area."

Given the range of threats and attacks, from phishing — the most common form of social engineering attack by individual opportunists — to state-backed cyber warfare, it is important to be aware of an attacker's level of competence.

Some attacks are unintentional, perhaps introduced by a USB stick; the 'standard' attacker will use hacking tools and techniques to gain access to a system; and the 'criminal' attacker will invest time and money to gather intelligence about the company, fleet or vessel.

The best line of defence begins when senior management takes responsibility at an enterprise level, builds a culture of security, and trains sea and shore staff in correct procedures. Cyber-security technology works best when the human element is in place.


Jochen Tack/Alamy Stock Photo

**Shipping companies are a target both for the value of their ships and cargo for ransoms, but also for their crucial role in supply chains.**

# State-backed cyber warfare concerns grow

The threat of rogue states — or criminals acting for them — cannot be ignored; but since states and criminals use mostly the same cyber tools, the damage they can do can be limited, **Declan Bush** reports

The threat of state-backed cyber attacks has returned with Russia's invasion of Ukraine — but how bad is it?

The conflict has already led to spoofing and satellite jamming in the Black Sea region and more is expected, with the Nato Shipping Centre and US Maritime Administration issuing warnings to shipping.

The infamous NotPetya ransomware incident, known to shipping as the Maersk cyber attack, began as a Russian assault on Ukraine that spiralled out of control.

The escalating tensions carry a risk of more cyber warfare, as well as the conventional sort.

Risk Intelligence analyst Kristian Bischoff said Russia would use cyber tools to secure manoeuvring space — to know where its ships were, while keeping that knowledge from its foes.

> *"You can affect economies significantly by undermining confidence in their marine infrastructure, whether it's the ports, the terminals, the ships, the logistics train"*
>
> **Bill Egerton**
> Chief cyber officer
> Astaara

Bill Egerton, chief cyber officer at Astaara, a cyber insurer, said while there is little good data on incidents, he has seen a sharp rise in cyber attacks with a war-like or terror character, and with a motive other than financial gain.

"Systems are being damaged, sensitive data is being exfiltrated and, while responsibility is not being admitted, there is clear evidence that tools and techniques are being deployed that are known to be used by groups with known links to nation states," he wrote in February.

Access course | BSc | BSc (Hons) | MSc

# SUSTAINABLE MARITIME OPERATIONS

## PART-TIME DISTANCE LEARNING

MLA COLLEGE

FLEXIBLE PAYMENT - STUDY ANYWHERE IN THE WORLD

THREE INTAKES PER YEAR: JANUARY | MAY | SEPTEMBER

OTHER PROGRAMMES: HYDROGRAPHY | ENGINEERING | MBA

mla.ac.uk info@mla.ac.uk +44 (0) 203 997 7555

Attack vectors included compromised emails, exploitation of satellite communications, the use of remote access for updating third-party IT systems on board, using unsupported software, and improper use of USB sticks.

Mr Egerton told Lloyd's List that shipping companies are a target both for the value of their ships and cargo for ransoms, but also for their crucial role in supply chains.

"You can affect economies significantly by undermining confidence in their marine infrastructure, whether it's the ports, the terminals, the ships, the logistics train," he said.

He pointed to attacks on Daewoo Shipbuilding & Marine Engineering last year, and on Iran's Shahid Rajaee port terminal in 2020, as having "a fingerprint which is more than just your average drive-by shooting".

CyberOwl chief executive Daniel Ng said while his customers are increasingly concerned about the possibility of war, he estimated 95% of attacks were still "opportunistic criminal activity, rather than nation state".

However, he said the massing of ships could hurt navigation in the Black Sea, since a GPS signal weakens if it is spread between many ships in the same area, and priority is given to warships.

"As we start getting more of a build-up... there's always the risk of a spoofing or jamming capability, but also a bit more basically, there is just an increased risk of disconnection," Mr Ng said.

Allianz global cyber experts leader Rishi Baviskar said targeted attacks were harder to detect. Attackers could wait for years before striking and did not advertise their presence by demanding money.

Mr Egerton said while attacks on operational technology are reported to have increased in recent years, a company's head office can often be more vulnerable than its ships.

"If you want to attack an engine management system, you've got to know your onions," he said. "But if you want to attack an IT system, you can buy a kit off the dark web and have a go and see where you get."

Yet while state-backed attacks can cost companies millions, their powers to harm ships should not be mythologised. A ship with a jammed or spoofed satnav can still navigate the old-fashioned way if needed.

Not all attacks cripple their targets either; some seek only to steal processing power to mine Bitcoin without the target's knowledge.

Mr Bischoff said there were limits to what cyber can do in war and its threat was often overhyped.


**A criminal cyber attack shut down South Africa's port of Durban in July 2021.**

> *"As we start getting more of a build-up... there's always the risk of a spoofing or jamming capability, but also a bit more basically, there is just an increased risk of disconnection"*
>
> **Daniel Ng**
> Chief executive
> CyberOwl

Last year, reports said Iran had worked out how to hack ballast tanks to let in so much water as to tip over the vessel. Yet Mr Bischoff said driving it full steam ahead then pulling a sharp U-turn would do the same trick — and, at any rate, Iran was "capable of punching holes in ships whenever they want" with missiles.

States could cause more harm by disrupting port operations than interfering with ship movements, he added.

While the other weapons available to nation states far outclass those available to criminals, cyber attackers use mostly the same tools.

Mr Bischoff noted that a criminal cyber attack shut down South Africa's port of Durban in July 2021.

"The interesting thing is that whether or not it's a criminal or a state, the outcome will be the same," he said.

This means the threat is wide-ranging, but also limited. Even NotPetya exploited known vulnerabilities and was delivered through an update from an otherwise trustworthy supplier.

And, while a company may not be able to do much about a targeted attack by a foreign spy service, such services are less likely than criminals to target shipping companies unconnected to national conflicts.

As with the Covid pandemic, there is a risk of new cyber variants emerging, against which the community has no protection. Yet like Covid, the same protective measures work for most of the viruses circulating in that community.

"By doing the basics properly, you get a lot of protection," Mr Egerton said.

## Shipping wakes up

Shipping's cyber awareness is improving slowly, helped by the IMO2021 call for ships to plan for it in their safety management systems and by the steady increase in incidents as companies learn vigilance the hard way.

Flag state authorities like the US Coast Guard have actively enforced the new IMO requirement. The International Association of Classification Societies is looking at how to harmonise different responses to it.

Governments are becoming less tolerant of breaches, especially of personal data. However, they need to be better at advising on best practice, to stop companies that skimp on security from distorting the market with artificially low prices.

Owners are also looking at how much to insure against cyber risks. And they are increasingly mulling whether to separate their cyber-security operations from the rest of their IT departments, so the former can better police the latter.

Mr Ng said the industry is talking about the topic differently than even a year ago: "People are just waking up to the idea that they've got to do something about it."

However, there is a gap between those on shore and at sea: 83% of shore-side employees feel close to ready for an incident, but just 37% of seafarers feel the same, a survey of 200 companies found.

It found the average cost of cyber attacks to operators was about $1.8m a year — including costs of paying ransoms, mediation, and bringing hacked systems back online — while companies spent just $100,000 a year on cyber security.

> *The interesting thing is that whether or not it's a criminal or a state, the outcome will be the same*

**Kristian Bischoff**
Analyst
Risk Intelligence

> *If you want to save some losses, you have to invest money and time*

**Rishi Baviskar**
Global cyber experts leader
Allianz

Mr Egerton said companies find it hard to calibrate how much to pay because of the perceived disparity between the risk and return of cyber security.

Cyber risk remained an alien concept to most people. Human factors like improper use of personal devices could run a coach and horses through security policies, he added.

The only safe option was for companies to assume they would be hit, work out how much they could lose, and how much they were willing to invest to reduce that amount. Good cyber defence is not a one-off purchase, but a change in how companies do business.

Mr Baviskar said crew training, including scenario testing, was important — as was segmenting a company's IT operations to diffuse the risk.

And better "cyber hygiene" did not mean upgrading everything at once. Companies should protect their crown jewels first and review their cyber security regularly, he said.

"We've seen companies moving towards that. But again, if you want to save some losses, you have to invest money and time."

# Cyber-risk cover: not as easy as you would think

In principle, it should be straightforward to come up with insurance products that cover those in the maritime industry in the event of a cyber attack; in practice, it is harder than you would think, **David Osler** reports

Aleksandra Chalova/Alamy Stock Photo

**Major charterers are increasingly asking shipowners to evidence the level and scope of their cyber-assessment processes.**

The past five years have seen a spate of cyber attacks on big names in the maritime industries, with victims including Maersk, Clarksons, CMA CGM, HMM, MSC and even the International Maritime Organization itself.

Companies have found themselves substantially out of pocket; the hit to Big Blue in 2017 may have been anything up to $300m.

There has yet to be a major casualty at sea that can directly be attributed to cyber events. However, most experts consider that only a matter of time.

In principle, any shore- or ship-based electronic, navigation or computer system is vulnerable to the unwanted attentions of hackers, be they hobbyists, criminals or terrorists.

There need not even be malevolence at work. A lost laptop or an unencrypted email can result in a serious breach of security.

Certainly such exposure is becoming a concern of major charterers, who are increasingly asking shipowners to evidence the level and scope of their cyber-assessment processes and the control, mitigation and recovery plans they have in place.

The issue should not be beyond the ingenuity of the marine insurance sector to resolve, and bespoke products are already available. Yet the process has not been as straightforward as it should be.

To begin with, underwriters cannot agree among themselves as to whether cyber is best written in a marine book, a political risks book or a bespoke cyber book. Everyone seems to have a different view.

Then there is the relatively new nature of cyber attacks, which did not exist until recent times. Without historic data, it is difficult for underwriters to build actuarial models that quantify and price the risk.

Indeed, there has been a natural tendency on the part of insurers to overprice cyber — which, unsurprisingly, has inhibited uptake.

The Catch-22 is that the embarrassment factor has meant some companies have not publicly divulged cyber attacks. That makes it difficult for the underwriters to obtain data as a basis for quotes in the first place.

James Cooper, managing director of one the few marine cyber specialists, Astaara, describes this as being a key problem when the company was set up.

"As a good, prudently regulated business, we had to understand what we were pricing for and why we were pricing for what we were doing. There was not enough data around," he said.

Fortunately, surrogate yardsticks could be developed by methods long established in the insurance industry. Variables such as the cost of replacing a ship's control panel are already 'known knowns' from the hull portfolio, and can be replicated across the sector.

Where the decision is taken to write cyber as part of a marine book, another problem is getting the wording right. The old Institute Clause CL380, introduced in 2003, specifically excluded cyber risk and was widely derided as hopelessly out of date in the modern world.

RGB Ventures/SuperStock/Alamy Stock Photo

**Hull insurance typically covers up to 65%-75% of value, and owners buy increased value (IV) as a bolt-on in the event of total loss.**

## Blanket exclusion clause

In 2019, it was replaced with the Lloyd's Market Association's LMA5402, also a blanket exclusion clause, and LMA5403, which covers non-malicious cyber risk but excludes malicious cyber attacks.

There is a body of opinion that neither marks much of a step forward. It is difficult to point to a cyber attack that does not involve an element of malice somewhere down the line.

Some also feel that LMA5403 does not define either 'malice' or 'harm' sufficiently sharply, which is a signal drawback for a clause of this type.

The International Underwriting Association approach is to look at whether the loss was directly or indirectly caused.

"I think the LMA approach is being preferred in the market for those who want to write non-malicious cyber, though of course this would still leave you without cover for malicious cyber, which is effectively war or terrorism," pointed out a lawyer at a London law firm specialising in marine insurance.

Even with specialist products, some question the appropriateness of the limits available. Typically, limits for broad-based cover remain at around $5m or $10m, and going higher than that limits the range of insured risks.

"There's another way of looking at this," argues Mr Cooper.

"Hull has traditionally bought full value insurance. But even within hull insurance, you have the main hull product and then you have the IV [increased value] product."

Hull insurance typically covers up to 65%-75% of value, and owners buy IV as a bolt-on in the event of total loss. That is low probability and therefore priced accordingly. More than 90% of hull claims are of less than $10m for attritional losses.

"People don't need high-value limits. We know other insurers can offer higher limits, but they offer very little cover," said Mr Cooper.

"The cost of paying for a loss, whether it is caused by a hull or a cyber event, will be the same. We know that the loss value is unlikely to breach $10m for a single vessel."

> *"As a good, prudently regulated business, we had to understand what we were pricing for and why we were pricing for what we were doing. There was not enough data around"*
>
> **James Cooper**
> Managing director
> Astaara

## Insurance budgets

People want higher limits, without a doubt, he added. However, until a couple of years ago, shipping company insurance budgets were not even taking cyber into account.

Hull, P&I, combined general liability cover and directors' and officers' cover are mandatory, and getting more expensive. Cyber remains optional, and is a new product.

So for now, the uneasy compromise remains between owners crossing their fingers, those taking the basic cover and those going for the full package. The market is yet to settle on which strategy will prevail.


Rawf8/Alamy Stock Photo

**The wider world has come to know the top five cyber risks: ransomware, phishing, data leakage, hacking and insider threats.**

# Modern three Rs: ransomware, recommendations and regulation?

High-profile incidents of cyber crime within the maritime sector led the IMO to publish its cyber-security recommendations; maybe now it is time for shipping to wake up and address cyber threats, writes Hill Dickinson LLP's **Mark Weston**

High-profile cases of cyber attack on some of the shipping industry's largest companies have raised awareness of the potential impact of cyber crime and the need for both up-to-date security systems and emergency planning procedures.

Merchant shipping is increasingly reliant on the transfer of data from ship to shore, particularly to monitor vessel efficiency and to demonstrate compliance with increasing global environmental regulations.

However, the digital connections between a ship and its owner can become a weak link if cyber security is not considered.

The risks are numerous, ranging from the infection of operating systems by malware introduced accidentally via a crew member's laptop or internet link, to deliberate attacks that seek to compromise a vessel's data or disable its operations.

These risks led to the introduction of comprehensive cyber-security recommendations last year by the International Maritime Organization.

This action has raised awareness of the potential risks that need to be mitigated — but the maritime industry still lags behind many of its land-based compatriots when it comes to understanding the cyber sphere.

The wider world has, unfortunately, come to know the top five cyber risks: ransomware, phishing, data leakage, hacking and insider threats.

There are many others and they have become part of business risk assessments worldwide. If you do not know what any of these are, you should be popping the terms into your nearest online search engine.

Gradually, many businesses in other sectors are implementing various standards regarding IT and information security designed to allow method, policy and process routes to attempt to stop — or, at the very least, reduce the risk of — all of these five threats.

For example, ISO/IEC 27001:2013 (usually better known as ISO27001) is the international standard that sets out the specification for an information security management system.

It uses a best-practice approach aimed to help organisations manage information security by addressing people and processes as well as technology. There are others, too.

The pandemic has shone a light on the role of digital systems to enable business continuity and the importance of back-up systems with robust cyber security.

Today's maritime sector is particularly prone to attack as technology becomes ever more widely used and data — whether it is about cargo, staff, location, weather or vessel monitoring — becomes increasingly important and transportable, and able to be corrupted, exploited or stolen if in the wrong hands.

Identifying risk is a sobering exercise. Think about the potential to hack or intercept the remote signal between a vessel and its office; the risks to vessel safety of someone interfering with GPS co-ordinates; the risks to environmental compliance or performance monitoring of a cyber criminal gaining access to vessel sensors and corrupting them or triggering false alarms.

In 2020, the United States Maritime Transportation System, in association with the Information Sharing and Analysis Center, issued its first-ever general warning to all tug owners, advising that their connected operations were vulnerable to cyber attacks — whether they be state-funded hacks, malware hits, virus infections or any of the other myriad cyber threats out there.

That warning was prompted by a phishing email, which was sent to a maritime facility, that had a voicemail attached, imitating a vessel operator. Fortuitously, this was caught and notified to an agency dealing with cyber threats who then alerted MTS-ISAC.

After analysis, the report found that one of the HTTP requests in the email was too sophisticated to be flagged by any known threat detection solution.

There were other sophisticated hallmarks, perhaps too technical to go into here — but suffice to say, it involved an IP address geo-located to Germany.

Those aware of growing dangers to the maritime world will know that the IMO's Facilitation Committee and the Maritime Safety Committee approved new guidelines on maritime cyber-risk management that superseded interim guidelines that had been in place.

> *Today's maritime sector is particularly prone to attack as technology becomes ever more widely used and data... becomes increasingly important and transportable, and able to be corrupted, exploited or stolen if in the wrong hands*

**Mark Weston**
Partner, head of commercial (London)
Hill Dickinson LLP

Coming into effect in January 2021, these guidelines provide high-level recommendations on maritime cyber-risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities, and include functional elements.

For development and implementation of specific shipping risk management processes and systems, the guidelines are intended to be supplemented by requirements of specific member governments and flag administrations, as well as relevant international and industry standards and best practices.

Many of these are yet to be published; as we know, shipping is often a late-adopter when it comes to technology and regulations.

However, every organisation in the shipping industry is different and the guidelines are expressed in broad terms to have a widespread application; the more complex an entity or its systems, the more care and resources are expected to be expended.

Yet a shipping business does not want to be the most secure, compliant — and insolvent — entity in existence. As with so many areas of law, compliance and regulation, it is about reasonableness and proportionality.

The guidelines are recommendatory only — but there is a sting in the tail (more of that later).

The guidelines contain a non-exhaustive list of vulnerable systems, including bridge systems; cargo-handling and management systems; propulsion and machinery management and power control systems; access control systems; passenger servicing and management systems; passenger-facing public networks; administrative and crew welfare systems; and communication systems.

They also make the important distinction between information technology systems (which focus on the use of data as information); operational technology systems (where that data is used to control or monitor physical processes); and interfaces that allow exchange of information within and between such systems.

They also note possible vulnerabilities at every stage of the acquisition and implementation chain, from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyber discipline.

That latter issue is often direct (for example, weak passwords allowing unauthorised access) or indirect (such as the absence of network segregation). All these have implications for security and the integrity, confidentiality and availability of information.

Most important of all, these have implications for safety — particularly where critical operations, such as main propulsion systems or bridge navigation, are compromised.

The lack of mandatory status is because a mandatory set of rules would be out of date extremely quickly as technology changes and as new threats develop. Accordingly, the approach taken by the IMO is — as in so many other industries — a resilient and evolving risk-management approach to cyber risks, which is a natural extension of existing safety and security management practices.

One of the biggest issues in cyber-risk management is ensuring that management appreciates the importance of it and is willing to expend resources (read 'cash') to put the necessary preventative measures in place.

This can often be perceived as spending money to stand still — but in reality, it is about mitigating risk so everyone can sleep at night (on the high seas or otherwise)!

The guidelines reflect this by making clear that: "Effective cyber-risk management should start at the senior management level. Senior management should embed a culture of cyber-risk awareness into all levels of an organisation and ensure a holistic and flexible cyber-risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms."

It comes down to the oft-quoted compliance refrain of policies, procedures and process. A key part of this is appropriate training at all levels of the business; everyone has a responsibility for security.

So, for those who have not yet embraced the IMO guidelines, where should a maritime business start?

The guidelines do not spell it out as clearly as I am about to, but any compliance plan should start with the creation of a snapshot as to where an organisation is at; then a plan for where it needs to get to; and the gap is then plugged with a costed, detailed remediation plan.

The plan should be RAG-coded so resources are spent on the 'red' areas first before moving to 'amber' and then 'green'.

The non-sequential functional elements suggested by the guidelines are:

**1. Identify:** The need to define personnel roles and responsibilities for cyber-risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

**2. Protect:** The need to implement risk-control processes and measures, and contingency planning to protect against a cyber event and ensure continuity of shipping operations.

**3. Detect:** The need to develop and implement activities necessary to detect a cyber event in a timely manner.

**4. Respond:** The need to develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber event.

**5. Recover:** The need to identify measures to back up and restore cyber systems necessary for shipping operations impacted by a cyber event.

agefotostock/Alamy Stock Photo

**The IMO guidelines contain a non-exhaustive list of vulnerable systems, including bridge systems; cargo-handling and management systems; power control systems.**

> *"It comes down to the oft-quoted compliance refrain of policies, procedures and process. A key part of this is appropriate training at all levels of the business; everyone has a responsibility for security"*

And what about that sting in the tail that I mentioned? Despite the guidelines only being recommendations, since January 1, 2021, by Resolution MSC 428(98), the IMO has required cyber security and risks related to be tested in audits; essentially, an organisation must demonstrate that cyber security is an integral part of the safety management systems being used.

In short, it is important to:

- Identify objectives in the field of cyber security;
- Undertake a mapping exercise of existing systems, software, policies, procedures and processes;
- Undertake a gap analysis of the differential between where the current map shows you are and where you need to be in terms of your objectives. This gap analysis then needs to be turned into a costed and step-by-step remedial plan. This will probably include:
  - Ensuring management buy-in and allocation of key roles and responsibilities for cyber security all the way to management level;
  - Putting in place or upgrading cyber-security policies and procedures. These need to be workable and used and not just a tick-box exercise or "something you have to have";
  - Upgrading networks, segregating and hardening them;
  - Training, training, training of everyone in the organisation, appropriate to their level. This should be both general awareness training and more specific role-based training; and
  - Implementing hardened systems and network segregation.
- Finally, it is vital to ensure that there is also a rolling programme of ongoing compliance and ongoing training so that cyber security is not just "something we checked" but becomes part of "business as usual".

Cyber threats are evolving — and so should you!

*Mark Weston, who is partner, head of commercial (London) with Hill Dickinson LLP, specialises in digital crime*
*This article was first published in Lloyd's List's sister publication, iLaw*


Posidonia
6 - 10 June 2022
Metropolitan Expo, Athens Greece
www.posidonia-events.com

Brain light / Alamy Stock Photo

**Supply chains are tightly connected by their nature, meaning an attack on one link can affect others.**

# Links in supply chain make perfect viral vectors

The increasing digitalisation and connectedness of containerised supply chains puts them at system-wide risk in the face of cyber attacks, **James Baker** reports

The relationship between container shipping and Russia's intentions towards Ukraine may seem somewhat tenuous, but bear with me.

While truth might be the first casualty of war, the initial fighting starts these days not on the battlefield but on the internet.

In the lead-up to Russia's invasion, this took the form of cyber attacks on two of Ukraine's banks and its defence ministry.

Neither of these are related to shipping — but nor was a similar attack on the Ukraine tax office in 2017, which installed the NotPetya ransomware on its systems.

And that virus was able to spread from there to the local offices of Maersk — and then on to Maersk's wider global network.

> *"Bring down a line or bring down one or two major ports and the mess we have now will look like nothing compared to what could happen"*
>
> **Lars Jensen**
> Chief executive
> Vespucci Maritime

It ended up shutting down several of APM Terminals' facilities for a week and cost the company hundreds of millions of dollars to rectify.

Little wonder, then, that Vespucci Maritime chief executive Lars Jensen puts the high risks of cyber attacks on critical infrastructure from the Russia-Ukraine conflict near the top of external shocks that could affect containerised supply chains over the coming year.

"Nobody even targeted Maersk; they were purely collateral damage," he said.

Back then, the market could handle the world's largest carrier being out of action for a week because there was buffer capacity in the system.

"Right now, there is zero capacity," Mr Jensen said.

## Container Tracker

# Save time. Stay compliant.

### Track containers, not just ships

Simplify transhipment tracking with end-to-end downloadable data trails on containers – by container number or Bill of Lading.

### Complete checks in minutes, not hours

Save time, with all the data you need in one interface, supported by tracking intelligence from over 600 Lloyd's agents worldwide.

### Download the evidence

Downloadable reports ensure you have the necessary documentation to prove compliance, including specific end-to-end transhipment reports and more.

Request a demo:
America Tel: +1 212-520-2747
EMEA Tel: +44 20 7017 5392
APAC Tel: +65 6505 2084
lloydslistintelligence.com/containertracker

Lloyd's List Intelligence

"Bring down a line or bring down one or two major ports and the mess we have now will look like nothing compared to what could happen."

Maersk is not the only carrier to have been affected by cyber attacks. CMA CGM, Cosco and MSC have all also been hit in recent years.

Even as this report went to press, US logistics major Expeditors announced that it had been hit by a cyber attack on February 20. It was forced to shut down most of its operating systems globally to protect the business.

At time of writing, the severity of the attack was still unknown, but Expeditors warned that, depending on the length of the shutdown of its operations, the attack could have a "material adverse impact" on its business, revenues, results of operations and reputation.


**In January, the port of Los Angeles launched its Cyber Resilience Center.**

## Digital crime

In an increasingly digitalised business, the impact of digital crime should be a growing concern.

So it is something of a shock to discover a new report revealed that despite a rise in cyber attacks during the supply chain crisis, 16% of UK businesses had deprioritised cyber security last year amid the pandemic, port closures, HGV driver shortages and other challenges associated with Brexit.

The report, commissioned by freight insurance specialist the TT Club from cyber-security firm Kaspersky, found that both large enterprises and smaller business were showing a "worrying level of complacency" when it came to protecting the resilience of their supply chains.

The complex relationships in supply chain management mean the infiltration of any one organisation can affect many others.

"If one of these entities has low cyber-security threat protection — or it is avoiding some specific cyber-security hygiene protocols — it could become the entry point into a much wider network of suppliers," the TT Club said.

"If a supply chain's weak link is exploited, a business can be brought to its knees."

That thinking is what lies behind developments at the port of Los Angeles, which, in January, launched its Cyber Resilience Center.

Described as a "state of the art" port community cyber-defence system, the CRC was created to improve the cyber-security readiness of the port and enhance its threat-sharing and recovery capabilities among supply chain stakeholders.

> *"We must take every precaution against potential cyber incidents, particularly those that could threaten or disrupt the flow of cargo"*
>
> **Gene Seroka**
> Executive director
> Port of Los Angeles

"We must take every precaution against potential cyber incidents, particularly those that could threaten or disrupt the flow of cargo," said Port of Los Angeles executive director Gene Seroka.

"This new Cyber Resilience Center provides a new level of awareness for our stakeholders by providing enhanced intelligence, better collective knowledge-sharing and heightened protection against cyber threats within our supply chain community."

Christopher McCurdy, general manager of IBM Security Services, which manages the centre, said: "The past year has proven the vital role that ports hold to our nation's critical infrastructure, supply chains and economy, underscoring that it is paramount we secure this ecosystem."

The CRC enables participating stakeholders to automatically share cyber-threat indicators and potential defensive measures with each other.

This collaborative approach centralises threat information for the port's supply chain participants and should help prevent cyber disruption of the supply chain. The CRC is also available to participating stakeholders as an advisory resource to assist with recovery.

## Sharing of information

This collaboration and sharing of information was also behind guidance from the Digital Container Shipping Association's cyber-security implementation guide, designed to facilitate vessel readiness for the International Maritime Organization's Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems.

"As shipping catches up with other industries, such as banking and telco, in terms of digitisation, the need for cyber-risk management becomes an imperative," said DCSA chief executive Thomas Bagge.

"Due to the global economic dependence on shipping and the complex interconnectedness of shipping logistics, cyber attacks such as malware, denial of service, and system hacks can not only disrupt one carrier's revenue stream, they can have a significant impact on the global economy.

"As a neutral digital standards organisation, DCSA is uniquely positioned to help vessel owners mitigate the increasing risk of cyber attacks on their ships — and, in turn, on the industry at large."


# Get a complete view from the trusted source for maritime data and intelligence

Connect to your target audience with engaging content and realise new opportunities to drive revenue

Valuable ownership data providing a full understanding of your customers

Consultants providing a future view of the world fleet to help you grow your business

Verified intelligence on capacity and trade route changes helping you discover new opportunities

## Choose the trusted source

Contact us today on **+44 20 7017 5392 (EMEA) / +65 6508 2428 (APAC) / +1(212) 502 2703 (US)** or visit **lloydslistintelligence.com**


# Get a complete view from the trusted source for maritime data and intelligence

80+ expert analysts review, analyse and enhance data to give you the most validated view

Consultants provide you with the future view of the world fleet

Connections with key industry players provide you with exclusive news and insight

## Choose the trusted source

Contact us today on **+ 44 20 7017 5392 (EMEA) / +65 6508 2428 (APAC) / + 1(212) 502 2703 (US)** or visit **lloydslistintelligence.com**