Issue 6. January 2015 | Quarterly

futurenautics

the maritime future

Sentient Ship | Cyborg Crew | Shipistics | Business e-volution

seaworthy?

Shipping's new security paradigm.

Image credit © Getty Images

Hope and Prey

The devil may take the hindmost, but cyber-criminals are taking everyone, and shipping looks like easy prey. We need a new security paradigm, and setting it isn't IT's job. It's yours.

There's an old joke involving a couple of wildlife documentary film crew, hunkered down in the African savanna filming lions. Suddenly a big male lion spots the two men and roars threateningly. As the soundman slowly starts to pull on a pair of Nikes the cameraman whispers to his friend that he'll never outrun a lion. To which the soundman replies that he doesn't need to outrun the lion, just the cameraman.

When it comes to cyber security, up until comparatively recently, the objective of the exercise has been to outrun the cameraman. For most organisations the risk of finding themselves exposed on the savanna in the first place is considered pretty low. That their digital assets would constitute anything juicy enough to interest an aggressive predator has been judged highly unlikely. So strapping on some Nike firewalls and antivirus and locking down the perimeter of the organisation seemed the sensible thing to do. Because there will always be some other slower, easier target for the hackers.

It is difficult to overstate just how dramatically that paradigm has changed. But it's dramatic enough that at the recent World Economic Forum in Davos fears were raised—both publicly and privately—that concerns about corporate cyber vulnerability are beginning to act as a brake on technology investment, and failing to address it could cost the global economy US$3 trillion.

The cyber security threat landscape has metamorphosed into something entirely different, and outrunning the cameraman is a woefully inadequate response. Now the internet is that savanna, and anyone on it is exposed. In addition the lion is able to maul an unlimited number of wildlife documentary film crew in one go with such stealth and savagery that they may not even realise they've been mauled until they attempt to make use of an internal organ and discover it's no longer in situ. And with the biggest vulnerability now your own people, the sound guy is just as likely to get eaten by the cameraman.

When writing about cyber security it's easy to get sucked in by the numbers. They're big. Really big. And they're getting bigger all the time. Try this one—last October JP Morgan suffered a data breach which affected 76 million customers. Or what about mobile payments provider CHARGE Anywhere which in December revealed a malware attack on its electronic payment gateway systems which had lasted five years. The statistics are jaw-dropping and you can read a judicious collection of some of the most noteworthy in our infographic. But there's only one statistic I'd really like you to take away from all of this.

It comes from Cisco, and more specifically its Global Security Network which handles 100 terabytes of data and inspects 16 billion web requests per day, has 100 million globally deployed endpoints, 1.6 million globally deployed devices and handles 35 per cent of all the email traffic in the world. The figure I want you to remember is 100 per cent. That represents the proportion of business networks analysed by Cisco which have traffic going to websites that host malware. Suspicious traffic is emanating from these company networks and attempting to connect to malicious malware hosts, which means that every company has shown evidence of internal compromise. Every single one.

Everyone is vulnerable and everyone is a target. But perhaps more salient is that as a board member you're also something else, and that is responsible.

So let's start by stamping on any lingering hopes—should you be harbouring them—that cyber security isn't really an issue for you. Everyone is vulnerable and everyone is a target. But perhaps even more salient is the fact that you, as senior leaders or board members of an organisation are also something else, and that is responsible.

As the tone in Davos indicated the severity of the threat and the ability of companies to meet it is beginning to jeopardise the significant economic gains that technology can offer the world. The response from the USA and UK is the formation of joint 'cyber-cells' to test resilience and share knowledge and intelligence between the two countries, but while there are moves to help organisations fight back, there is also a regulatory tightening underway. Both the USA and Europe are introducing compulsory reporting legislation and companies who breach data laws, however unintentionally, are being handed significant fines. In short, ignorance is no longer a defence, and nor is unpreparedness.

That has serious implications for the shipping and maritime industry, because there's a good chance that we are massively—some would claim recklessly—unprepared for the new cyber threats we are facing. Wary of generalisation as I am, after the discussions I've had with a whole range of people around the industry on the subject, it does appear likely that on the whole we are neither secure nor resilient when it comes to cyber.

According to recently released 2015 security reports by both PwC and Cisco the volume of cyber attacks has mushroomed year on year, and continues to do so. Cisco Systems CEO John Chambers told a meeting in Davos that “security was bad last year” and unfortunately “this year is going to be much worse.” The good news is that the profile of cyber security within our industry is on the rise. The International Maritime Bureau and BIMCO have already issued warnings, and Canada's submission to IMO on the subject was also widely reported.

In the last year we've also begun to see more reports surfacing of successful attacks in the maritime domain. From drilling rigs having their control systems infected and Korean shipbuilders being infected with the 'Icefog' virus, to the Port of Antwerp and Australian customs being compromised by smugglers, evidence is emerging about the scale of attacks and potential vulnerabilities.

Thanks to a previously secret report from the US Senate’s Armed Services Committee, we now know that there have been multiple cyber attacks on ship operators and ships themselves contracted by the US Transportation Command (Transcom).

But the problem is that most of these reports are years old—the Transcom attacks happened in 2012/13—and

The high-profile hacking of Sony Pictures led to the cancellation of its film 'The Interview', but also leaked employee data into the public domain. Several have now launched a class action.

Image credit © Sony Pictures

considering the speed with which the threats are evolving, and the sheer scale of attacks that simply isn't good enough.

Despite all the statistics and the reports it is hard to really comprehend that scale. In order to get your head around it though I suggest that you visit the Norse website. Norse claims to have the world's largest up-to-the-second database of live threat intelligence, and you can watch live online, as literally thousands of attacks ping their way across the world. Actually what you're seeing is only part of the activity, but it's enough. If you haven't seen it yet then the advice from Dan Solomon—Consulting Lead for Cisco's Cyber Security Centre of Excellence and head of the Cyber Risk and Security Services division at Optimal Risk—to delegates at the recent Transport Security Expo's maritime conference that they need to go onto a 'war footing', may seem theatrical. It won't afterwards.

Experts divide the threat into four main groups—hacktivists, organised crime, company insiders (either intentional or unintentional) and state-sponsored entities—all of which is true. But that misses the fundamental point—the real essence of the cyber threat, and that is dependence. The only reason that we are vulnerable to these groups is because of our dependence upon the technologies we are implementing, and that's why the dangers are growing and the paradigm is shifting so fast.

Pre-digital organisations used to have solid perimeters, originally the walls of the office building. The advent of email and company laptops bulged them out, but the response was to beef up the firewalls and antivirus. This approach has been described as "M&M" security—a hard shell with a soft centre, where everything outside the network is untrusted and everything inside is trusted. But the explosion in social networking, the BYOD and ATAWAD trends and cloud collaboration platforms has sent it into meltdown.

According to John Kindervag, principal analyst at Forrester Research, that attitude to network security has become a fundamental problem. "The world has changed and we cannot carry on doing things the way we did in the 70s and 80s," says Kindervag.

That's exactly what shipping and maritime are still doing in lots of areas, and with good reason. The huge advances in connectivity which has forced land-based companies to evolve along with the new security landscape have been missing from the maritime domain. Now that high speed IP connectivity is not only affordable, but clearly the key to unlocking significant operational efficiencies, cost savings and service improvements, maritime is taking massive leaps forwards, but without an appreciation of the risks.

"Connectivity offers huge benefits and it's really important to understand that, but people have had quite a rosy picture of what those benefits are or could be and they haven't really considered the potential downsides," says Wil Rockall a director in KPMG's cyber security team. "Vessel cyber security is reasonably immature as the vast majority have paid more attention to physical security, which is only to be expected given the last ten years and where the attacks have come from."

So most ship operators are still dishing out M&M security, relying on the same firewalls and anti-virus, but even the people developing those products are warning they don't work. According to Symantec its firewall and anti-virus products will stop at most 45 per cent of threats getting through and Symantec's SVP Brian Dye went as far as to tell the Wall Street Journal that 'antivirus is dead'.

Actually saying that antivirus is dead is like claiming that an aspirin doesn't cure cancer. Antivirus may not be a panacea, but it is still useful as part of a suite of defences. There are a new generation of products like free software Comodo which provides a virtualised sandbox for users isolating them from the threat of viruses online, but in reality very few people actually come into contact with viruses these days. The far bigger threat is from malware, and that's usually just a user's click away.

For shipping and maritime the key is a shift in mindset, an appreciation of how the threat landscape has altered and why a 'Zero Trust' model of security is now necessary. That also requires an acceptance that no matter how good your security is, there is a very good chance that at some point you will be breached. So cyber security is only one part of a bigger requirement, and that is cyber resilience. The ability to identify the breach and recover is as crucial as mitigating the threat in the first place. Once we move from security to resilience it's easier to see that trying to protect everything, as we have in the past, is no longer the best option. In short the focus should no longer be on the network, but the data. We have to identify our key dependencies, our 'crown jewel' data. Then we have to work out how to deliver the right data to the right person on the right device in a secure way.

"Connectivity offers huge benefits and it's really important to understand that, but people have had quite a rosy picture of what those benefits are, or could be, and they haven't really considered the potential downsides," Wil Rockall, KPMG

That's why what may once have been an IT problem isn't any longer. This is a c-suite and board level issue, and what it comes down to in the end is risk. But while companies have elaborate models to measure financial and health and safety risks, and insurance products to help cover them, the same doesn't apply to cyber. By and large we don't have the ability to measure cyber risk and even less grasp of how we mitigate it.

It's safe to say that this is a pretty major issue. And yet when you ask those actually running shipping and maritime companies what they're doing about it the response is total silence—both about the scale of cyber attacks in shipping and maritime, and the work that is required and underway to mitigate them.

"Maritime is way behind the curve in standards on cyber-security," says Alex Soukhanov, vice president of international shipping and maritime operations at the United States Maritime Resource Center, a nonprofit consultancy specialising in navigation safety and maritime risk mitigation. "Traditional risk approaches are leading to common wisdom saying, 'where's the threat?' when the low level of reporting means we don't recognise the threat. But we have to remember that as mariners we're only as good as our last manoeuvre."

There's an argument which says that this could be 'Digital Darwinism' at work. Those who have failed to evolve solutions to the new threats technological changes sweeping shipping and maritime, and the rest of the world, are creating, will just go the way of the other dinosaurs. But the issue is far more complex than that. I imagine a lot of shipping and maritime companies will look at the Sony attack or that on the US Command Center's social media accounts, or Apple, or JP Morgan and conclude that any high-profile organisation with sensitive or valuable digital assets is going to be a target, which is precisely why the largely invisible shipping industry doesn't have too much to worry about.

Unfortunately that couldn't be further from the truth. The reality is that a big organisation's weakest link, after its own employees, is its suppliers. Cyber criminals are far from stupid and they will take the path of least resistance. Why try and breach a well-resourced, alert organisation with a lot to lose, when a smaller, less security-focussed supplier could provide an open door?

The problem is so acute that in other industries large suppliers have sometimes met the cost of upskilling and uprating the cyber security and resilience of smaller suppliers in order to mitigate the risk. But the evidence is that the problem is increasing. The recent PwC survey found that losses from cyber attacks jumped by 53 per cent year on year for large firms, but in small firms it decreased 37 per cent. The suggestion is that smaller firms simply aren't identifying when they've been breached, and when they are breached very often they aren't the ultimate target. Smaller firms are bridging the defences of their larger customers, letting the criminals inside, and they don't even realise.

The traditional M&Ms approach to cyber security—hard shell and soft centre—can't cope with the new business realities and is in meltdown. Symantec have declared their own anti-virus 'dead'.

Image credit: Plain M&Ms Pile by Evan Amos. Licensed under Public Domain via Wikimedia Commons

Considering that shipping and maritime sits at the heart of countless supply chains worldwide and its infrastructure includes support for everything from ports to oil platforms, the potential ramifications of that scenario in our industry is chilling indeed. This was demonstrated by a 'Red Team' exercise—a real-world approach to testing security, protocols, and awareness—conducted on a large port. (We cover Red Teaming in detail in our '*The Devil You Know*' article this issue)

Tasked with breaking into a port a Red Team of attackers got in via a shipping company web portal based in an underdeveloped part of the world.

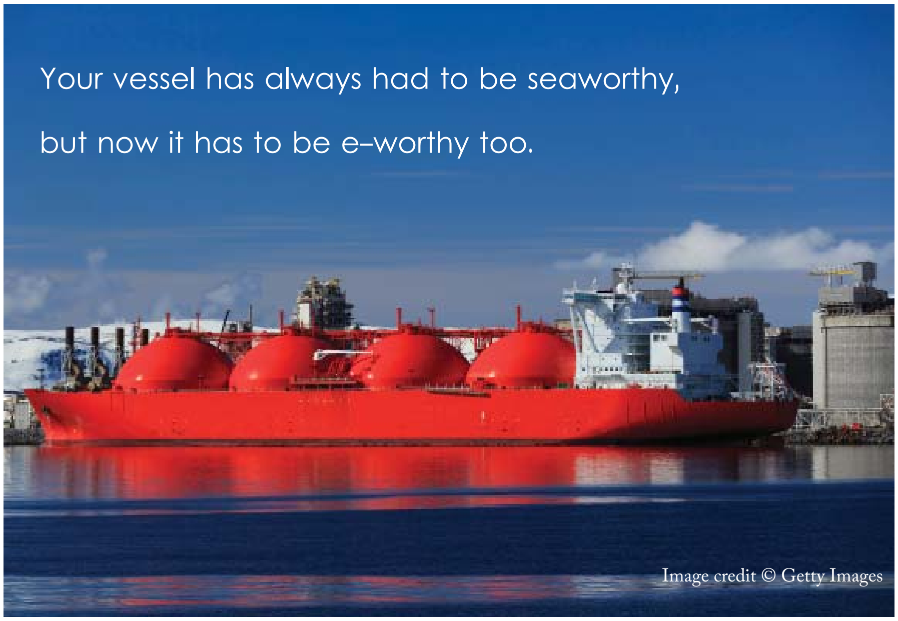
Tasked with breaking into the port and taking control of the network and systems the attackers found their way in by targeting the portal of a shipping company run from an underdeveloped country. I can't identify either the port or the large ship operator involved, but I can assure you that you will be very familiar with both.

If I'm doing my job properly then at this point you will be mentally running through the suppliers and customers you interact with on a regular basis, whose networks or devices your personnel might use when they visit, or allow to use your network when they visit you. And if you're doing your job properly you will be wondering the extent to which your organisation has vetted, and continues to vet, those companies' cyber security policies and procedures. The extent to which your organisation is exposed.

If the answer to your question is that you don't vet suppliers or customers, then you aren't alone. Despite the growing expectation for businesses to check their supply chains aren't engaged in bribery, corruption or employee exploitation, actually checking that they aren't going to compromise your cyber security barely registers. When one considers the extent to which every business deals online now that's an astonishing situation.

It may seem counterintuitive, but the safest place for shipping and maritime to trade online now might very well be a dedicated e-procurement platform. As a closely integrated EDI trading platform ShipServ is a de facto extension of its customer's systems and is seen as an additional layer of their data. Protecting that data, according to Founder and CEO Paul Østergaard, is a responsibility they take extremely seriously.

"We are dedicated to preventing, detecting, and responding to any threats that may target our infrastructure, and we are constantly working to protect our customers and their data," says Østergaard. "By continuously monitoring all activity, immediately responding to emerging threats and having an in-house security team and external security experts to test and improve our protection measures we are striving to provide the safest environment for maritime trade."


Your vessel has always had to be seaworthy,

but now it has to be e-worthy too.

Image credit © Getty Images

There's no doubt that ShipServ knows what it's talking about when it comes to data, and it operates a continuous cycle of evaluation and implementation of further encryption and data partitioning to prevent potential damage by cyber intruders. So for maritime companies without that security competence using the ShipServ platform could offer major risk mitigation. "This could be seen as a natural continuation of the deperimeterisation of individual customers' systems," agrees Østergaard. "We work with many thousands of customers and while some companies provide adequate protection for their systems and data, ShipServ remains a more secure option for the majority."

But while there are companies in maritime capable of meeting the challenges of the new cyber security paradigm, there don't seem to be enough, and we're rapidly approaching a crunch point. Increased connectivity is pulling every shipboard system possible online, converging and integrating functions and software and control systems.

Engines can be fixed remotely, images and video can be streamed and within a very few years we will have prototype ships that will sail themselves. Already our dependence upon these systems is heavy—the e-navigation agenda has made sure of that—but in future the safe and efficient operation of the ship at sea will depend upon them utterly. Your vessel has always had to be seaworthy, but now it has to be e-worthy too.

"Seaworthiness is very important concept in English Maritime Law, and is often central to disputes over marine Insurance and the carriage of goods by sea," says Christopher Dunn, managing partner at Waltons & Morse LLP and member of the British Maritime Law Association. "As vessels become more reliant on computer systems, cyber security vulnerabilities which are exploited by hackers, and which lead to physical loss of cargo or other damage, could form the basis of an unseaworthiness claim."

So if you put to sea with malware screwing up your ECDIS there's a very good chance your vessel could be con-

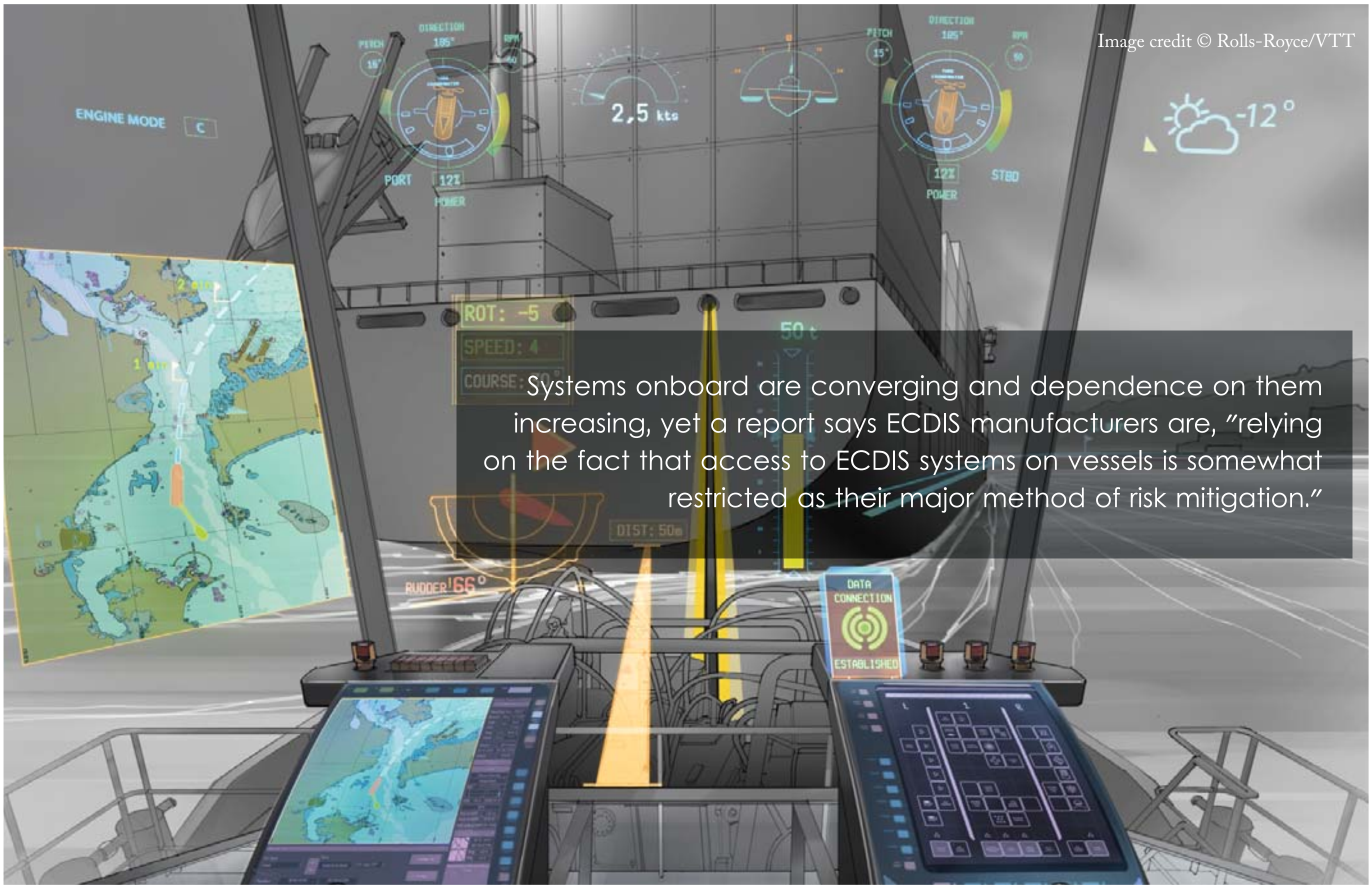


Image credit © Rolls-Royce/VTT

Systems onboard are converging and dependence on them increasing, yet a report says ECDIS manufacturers are, "relying on the fact that access to ECDIS systems on vessels is somewhat restricted as their major method of risk mitigation."

sidered unseaworthy. And that's not all. Most marine insurance policies Waltons & Morse see contain the Institute Cyber Attack Exclusion Clause (CL 380) which excludes all losses caused by or contributed to by a cyber attack. According to Christopher Dunn it's something that the industry is waking up to. "We are also seeing an increasing awareness that inadequately defended technical systems present huge risks and there is widespread unease that criminals, pirates and terrorists will gain access to these systems."

Unease is good, but perhaps outright fear would be more appropriate, particularly when you consider the evidence. NCC Group reported early last year on the vulnerabilities they found in an ECDIS from a major manufacturer. They were able to penetrate the system, read, download, replace or delete any file stored in it.

Access to the ECDIS could come from a virus on a USB stick, or an unpatched vulnerability via the IP connection, either directly, or through one of the other systems integrated with the ECDIS. In essence, once they were inside the ECDIS, they were inside the network and everything else connected to it.

NCC Group recommended that manufacturers adopt Security Development Lifecycles for ECDIS products, but it's rather alarming that a mandatory piece of shipboard kit wouldn't routinely have one. "Manufacturers are currently relying on the fact that access to ECDIS systems on vessels is somewhat restricted as their major method of risk mitigation," says the report." This is inadvisable."

But if the ECDIS research is scary consider the study security company IO Active undertook in 2013 directed at satcom terminals. Maritime terminals including Iridium, VSAT and Inmarsat FleetBroadband were reported as having critical security issues.

These were serious enough to be reported to the CERT Co-ordination centre, and yet according to IO Active, with the exception of Iridium, "the vendors did not engage in addressing this situation. They did not respond to a series of requests sent by the CERT Coordination Center and/or its partners." In a climate where everyone is becoming aware of how serious a cyber attack on a vessel, or a company could be, it seems puzzling to say the least that satcom terminal vendors and ECDIS manufacturers could have such vulnerabilities apparently present in their products, and it go virtually unreported.

As one of the major network operators, we asked James Collett, Director of Mobility Services at Intelsat what his network is doing to keep maritime users secure.

"We break the general security model into how we are protecting the perimeter and how we manage access to the network and for the elements of the system that are responsible for transport that we own, we maintain security measures on those," Collett explains. "Integrity of the network carrying customers' transmissions is of primary concern, and Intelsat is the only satellite operator that has gone through independent auditing firm KPMG and completed a Service Organization Control 3 (SOC3) review of security controls. The successful review process provides commercially accepted validation that our products are offered in an appropriately secure environment."

Intelsat spoke to us at length about this—and you can read the rest of what they had to tell us about security on our website—but in doing so they were in a very small minority. We also asked Inmarsat—responsible for the connectivity of the vast majority of vessels at sea and the only one anointed to provide GMDSS services—to tell us how they approached cyber security in the maritime domain.

Unfortunately Inmarsat doesn't discuss security. And they aren't alone. In shipping and maritime, no one wants to talk about cyber security. And I really do mean no one. For the purposes of this article we contacted more than fifteen large ship operators and numerous suppliers. None were prepared to talk about it on the record.

Organisations that work together to develop comprehensive defences are far more likely to remain secure than those who try and do it alone. Security should not be a competitive advantage.

Now we're used to people not wanting to answer the kind of difficult questions we ask—on a variety of subjects—but this is in a different league altogether. And it's a real problem, because the only way we're going to get on top of this is by sharing the information we have. In November 2013 the Bank of England held the 'Waking Shark II' exercise, designed to test the cyber security of the UK financial industry. It's something the maritime industry ought to consider and not just because of the vulnerabilities it could uncover.

James Collett of Intelsat, the only satellite operator who says its security has been independently audited and reviewed.

Image credit © Intelsat

Following Waking Shark Andrew Miller, chief operating officer at Corero Network Security, said one of the biggest benefits from the exercise will not necessarily be about banks learning to defend against cyber attacks, but learning to co-operate. “There needs to be more information-sharing within financial organisations on the latest threats and attacks they are facing, so they can develop a knowledge pool on how to protect against them,” he said.

Essentially those organisations that work together to develop comprehensive defences are far more likely to remain secure than those that decide to try and do it alone. The bottom line is that maintaining cyber security and resilience in the maritime industry isn't something that should form the basis of a competitive advantage.

"Keeping people safe, operating vessels safely should not be a competitive advantage for anybody, so there shouldn't be an incentive for any owner operator or manufacturer to keep that information to themselves," says KPMG's Rockall. "But at the moment we have two problems: one is that no one wants to be the first to admit they have a problem, come out and say they've been hacked and people were at risk, because the first person to put their head above the parapet is likely to get it shot off. Equally though, nobody wants to do the opposite and say we are perfectly safe and we've spent huge time and effort and we're confident we're secure, because that's painting a huge target on your back."

Whether or not ship operators and maritime suppliers talk to Futurenautics about cyber is of no consequence, but it is absolutely essential that they begin talking to each other. I think the real need here is for a co-ordinated response to the cyber threat, one which allows organisations to come together and share the intelligence they have, understand the problems that others are seeing and how they've overcome them. In that way we can protect and support each other and have a fighting chance of getting ahead of those sods on the other end of the IP.

If that sounds familiar it should: it's exactly what we did with physical piracy, and look at the results.

Someone said to me that when it comes to cyber and technology threats boards just glaze over. When you have seven year old girls hacking into public WiFi networks in under ten minutes you can understand why. In fact it reminded me of Douglas Adams' set of rules that describe our reactions to technology.

The first is that anything that is in the world when you’re born is normal and ordinary and is just a natural part of the way the world works. The second is that anything that's invented between when you’re fifteen and thirty-five is new and exciting and revolutionary and you can probably get a career in it. The third is that anything invented after you're thirty-five is against the natural order of things.

We don't need scaremongering, but that's inevitable when cyber is shrouded in such secrecy by everyone. What we do need is for those of you who lead our companies and boards to understand that cyber is not about IT, it is about dependence, and that dependence leads to risk. And like every other business risk, it has to be managed. That is your job, and you are perfectly capable of doing it successfully. But it's going to be a lot easier together.

So, unusually, I'm going to give the last word to someone else. In this case James Collett of Intelsat who told me, "When security is working correctly, it’s a partnership."

Yes. What he said.

Futurenautics is undertaking the first major research into how shipping and maritime boards are approaching the challenges of cyber security and cyber resilience. Take part at **www.futurenautics.com/maritimecyberwatch** and register to receive your free copy of the report.