SHIP MANAGEMENT INTERNATIONAL

Issue No 61 May/June 2016

Situations Vacant

BIMCO/ICS Manpower Report predicts more officer shortages

Security round table debate

In the latest of our industry round table debates, SMI drew together the leaders in global shipping to debate the one issue which is dominating discussion on the future role of technology in shipping – cybercrime. With the threat escalating, how prepared is shipping for this problem? Chaired by SMI Editorial Director ***Sean Moloney****, the panellists included* ***Esben Poulsson****, President of the Singapore Shipping Association and Vice Chairman of the International Chamber of Shipping;* ***Katharina Stanzel****, Managing Director of INTERTANKO;* ***Angus Frew****, Secretary General of BIMCO;* ***Rick Driscoll****, VP Operations, Mobile Broadband at KVH Industries;* ***Gerardo Borromeo****, President of InterManager and Vice Chairman of the International Chamber of Shipping;* ***Nigel Cleave****, CEO, Videotel;* ***Peter Hinchliffe****, Secretary General, International Chamber of Shipping (ICS);* ***Denis Petropoulos****, President of Braemar Asia; and* ***Viraj Nilakanta****, Business Development Manager, Fleet Management*

Sean Moloney
When it comes to cybercrime, who do we fear the most: hackers, competitors, seafarers with virus-laden personal devices, state actors or nations and why?

Esben Poulsson
With global terrorism and the sophistication that terrorists seem to have at the moment, when it comes to IT and modern technology I would probably say it is the terrorists we have to fear the most. Cybercrime is more serious than we all like to let on, because it is always very comforting to stick your head in the sand and hope that it is somebody else's problem. But I think a lot of the concern is based on a relative level of ignorance and, of course, the issue has come to the fore in relatively recent times. People are now beginning to take it seriously but I think it is going to be a very steep learning curve.

Viraj Nilakanta
From my perspective as a ship manager, our biggest threat in cybercrime comes from the hackers; those people are out there looking at it all from a commercial point of view. And we have had some experience of this where people have hacked into our systems, and sent a spam email with false information but with commercial implications to it. We had a situation where we had asked a client of ours for our management fee, but then someone hacked into our client's server and he sent nearly $300,000 to a scam account. After that, there was no trace of the money. So one of the challenges for us as a ship manager, is what protective measures do we take to ensure our safety; to ensure the ship's safety; and to protect our clients?

Sean Moloney
What measures can you take?

Viraj Nilakanta
What we did immediately was to tighten our systems up; so instead of sending invoices to our clients by email which can be infiltrated – we have a secure system where our clients can log in, so we send it through this system. We notify them that there is a request for money in the system for them.

Rick Driscoll
At a high level we fear all of these people, but at the level of the seafarer they may not even know they have a problem and they may bring devices onto the ship which can infiltrate the ship's systems and steal operational data, so as a satellite service provider we try and work with our customers to separate out crew devices from operational devices; separate out the networks and work to secure our network at a service level so the service has continuous operation but also so that the data going across all services is as pure as possible.

Sean Moloney
Are owners and managers complacent about all this?

Rick Driscoll
I think they are, most of the issues they have are that people are going to use the service too much. So they are worried about the cost of service versus the security of their data which is really surprising. So we try to work with them to help them to recognise these threats and prevent them.

Angus Frew
We, at BIMCO, have written, with our colleagues at the roundtable, some guidelines but they're really focused on the ship. We see the shore side as no different from any other commercial operation, and they have to put in place the same defences, but our biggest concern is what is happening on ships. I do believe there is increasing awareness but it is coming from a very low base; we put together the guidelines which are a risk-based approach, and are really looking to people to put in place the plans. But where are the biggest risks onboard at the moment? Our ships are generally pretty low-tech if you compare with many other transportation modes at this moment in time but there is a move towards much higher tech in the future as far as shipping is concerned. I think we are probably coming to exactly the right moment where our vulnerability is increasing. It was brought to my attention years ago that the risks to the ships were increasing because the cost of satellite communication technology has really significantly dropped so ships are more in contact with the shore than ever before, therefore the vulnerabilities are much higher. So where do I see the biggest risk and challenge and fears? It really comes from the crew and a lack of awareness of the issues and their behaviour. We should treat PCs onboard ships exactly the same way as we do on land. We should put the same protection around them such as passwords, so you don't have a general password pinned to the top of the PC which gives full administrative control of the computer. We need to update the software on these PCs on a regular basis, and we see that many ships are still operating on Windows XP which, quite frankly, is not sufficiently secure and you would not consider running that in your office. So we need to take the same values and behaviours that we have onshore onboard ships. Because a lot of ships are relatively low sophistication, engine management monitoring is something that is really just beginning but it is something for the future.

Sean Moloney
Are we just waiting for a big hacking incident because shipping is very good at reacting to situations?

Angus Frew
No, clearly there hasn't been a big incident. We have reacted ahead of the big incident and this is a very proactive approach in risk management.

Katharina Stanzel
Our biggest fear is not actually on your list, but one of the things we were just discussing in our safety and technical sub-committee two weeks ago is the risk coming through the service engineer when he is updating the software onboard and whatever critical systems he is working on. The guy with a ponytail and the boiler suit who nobody knows but who is suddenly on the bridge doing something to the ECDIS. Nobody is challenging him or asking what he's doing. So the assessment has to improve a lot and the equipment manufacturers that work with the shipyards. We must also consider the shipyards bringing out a new build with the equipment already installed onboard which has software that is actually three years out of date. We all know what it is like when there has been a Windows update, our entire office becomes unproductive for a day because the patches have done something to reset somebody's settings and introduce something that nobody knows how to work. It is these kinds of risks that for me, at the moment, seem to top the agenda because we are thinking about everything else. One thing I also feel very strongly about is that anybody over the age of 25 or 30 nowadays is a dinosaur when it comes to technology. The new generation of seafarers will have a completely different intuitive way of interacting with any kind of system and interrogating that system, and customising the system to make it do what they want. So we will have a paradigm shift in how people use technology onboard; there will be this discrepancy you see in some offices ashore where staff will go off and use the active system because they have learned how to use that system, and do what they think is best and then they have the older colleagues who will either have had training on a different system or on an older bit of software. This is where we

need more robust and wider reaching risk assessment so they can catch all of that. Cyber development is moving so fast nowadays; if we tie ourselves too closely into it we will miss stuff because it will have already developed by the time we have actually written and distributed the guidance.

Denis Petropoulos

I'm looking at all of this more from an operational perspective; a virus takes time to manifest itself at which time it is gone and it has happened. One of the points you mentioned here, is what are our responses? For me the biggest fear I have from cybercrime in shipping is an attack on ships' navigation systems. So we have a navigation attack you have to close it down, drive the ship by hand. And it is crucial because by the time you work out where your cyber-attack is you are on the rocks. That is a malicious cyber- attack but then of course you have cyber vandalism. We have people out there who have broken into NATO and now we're talking about ships but we will never beat it. We just have to figure out as a checklist on how we get around it. Nothing is more important to shipping and operation. We need to figure out how to handle it when the system shows there has been an attack.

Nigel Cleave

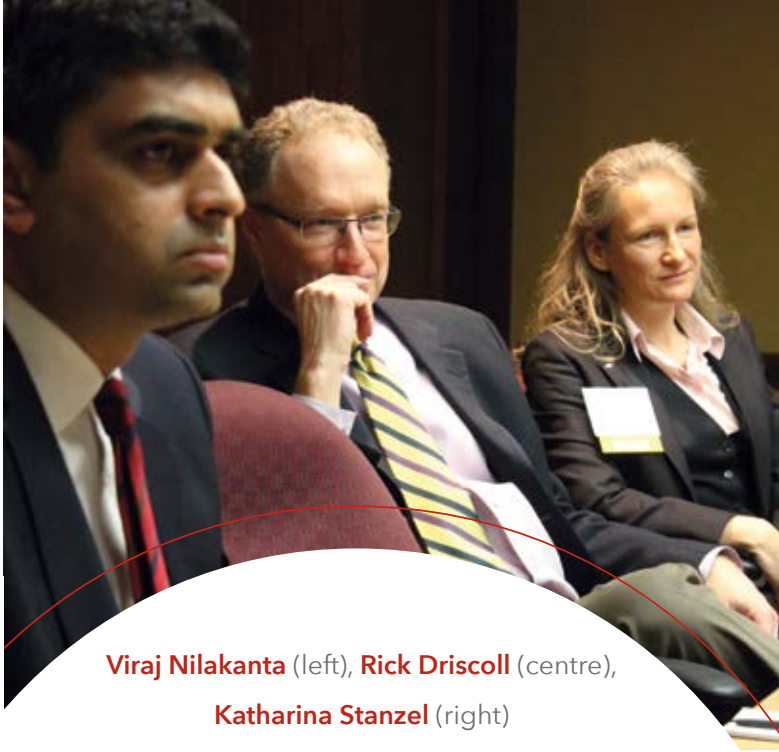
I think we have to be wary of all of these possible attackers. Whether it is for reasons of safety and protecting the ship or whether you have your crew with their USB sticks, using pirated material. Yes, communication is relatively low-level onboard at the moment but it is going to increase. Early this morning the Allianz safety shipping review 2016 said that more must be done to educate companies; cyber exposure is growing and they reckon that the Internet of Things, allied with increasing reliance on navigation, means insurers have less than five years to prepare for a cyber-attack or an incident materialising into a hull and machinery loss. So we have time at the moment but we have to be on our toes. We all remember Y2K, the industry stepped up to the plate then maybe we have to go that way again. Now we are even hearing about cargo manifests being hacked. So there has to be a set of rules and there has to be some form of regulation.

Sean Moloney

Is it also about changing mindsets onboard with the seafarers coming closer to the organisation rather than being this itinerant force?

Nigel Cleave

This is a new issue and shipping has to act quickly but it needs to act together. All the relevant stakeholders should work together to establish the correct safeguards. This needs to be directed through the IMO. It all starts with making sure onshore personnel and onboard seafarers alike have an awareness of how to use the Internet in a smart secure way that minimises risk – establish strong passwords, don't download questionable apps, don't open emails or attachments from unknown parties, etc; much of this can be handled through training.



Viraj Nilakanta (left), **Rick Driscoll** (centre), **Katharina Stanzel** (right)

Peter Hinchliffe

It is right to say that currently ships are, generally speaking, low-tech and so while the threat may be low we also have a high degree of complacency. As ships become more technologically linked to the shoreside, then we will have to address the complacency issue. To answer your specific question, I think there are two foremost threats - hackers for mischievous reasons and the other are seafarers because they simply don't know there is a problem there. Going back to the contractor issue, I don't see why we should be suspicious of a guy with a ponytail, because if the ship is compliant with the ISPS code than the guy shouldn't be on the ship anyway. We talk about all of this IT security but around the outside there is also the personnel security and if you do that then you will counter that problem.

Gerardo Borromeo

Rather than just talk about cyber security, we should focus on security in general. I have a fear when it comes to security; it is the fact that as we go about our day-to-day activities we often take things for granted because we trust, and when we trust that is when we have our greatest vulnerabilities. When you talk of security, whether it is cyber security or ship security, it is a fact that if anybody wants to do anything whether it's from a malicious point of view or more so if it is more purposeful reasons, we are up against many people who want to do bad things and our vulnerabilities are there. One way around this is to drive up education and awareness; it all has to be part and parcel of the checklist that Katharina was talking about. And unless it becomes a way of life we will never be able to overcome it and even as we try to overcome it, because we are playing defence, the offensive guys

are always going to be looking for the weakest link. At the moment the ship is a weak area only because of its level of technology but this weak area becomes an entry point for many things.

Sean Moloney
I want to talk about this issue of raising awareness and education. Esben what are your thoughts, is enough being done onboard ship?

Esben Poulsson
This is all individual to shipping companies but I know some shipping companies that have taken this matter much more seriously than others. I know companies who have departments focusing on this issue right now. But there is a sense of denial in some quarters so, yes, there is a problem but it is not really happening to me. It is a very mixed bag. In Singapore we are having a cyber security conference which is being organised by the MPA and the SSA and a lot of resources have been put into this conference reflecting the importance of the issue.

Gerardo Borromeo
We should look around and say how prepared are we to tackle this? We need to look at our own protocols. Only a couple of days ago I very nearly clicked on an email that would have had a virus on it. It is about recognising our ability to do something. How to train everybody in your organisation to be so careful so that it doesn't become disruptive in the day-to-day work they're doing, and this is what we are up against. It is no different than going through all the security we have to go through at airports. It causes disruption but despite all of the filtering systems, some things still get through. So what does that mean about vulnerability? I guess the other side would be if we have to spend time, it would be no different from the other scenarios that are done by ship managers who talk about risks. I just look at the stuff that comes into our offices and imagine how that can be replayed onboard ship where the administrative burdens on our offices are already such that fatigue can set in and they will click on this and click on that and who knows what will happen. If you have a vessel carrying cargo that is potentially harmful that is where the situation escalates even greater. I'm not saying there is no solution but it is a difficult challenge.

Angus Frew
The issue that we have to live up to is the fact that no system is going to be 100% secure no matter what you're doing; it is good to have to be reactive to a large extent because there are some very proactive people out there developing all sorts of ways to get into your systems. What our guidelines onboard ships set out to do, is identify where the biggest issues are and where your biggest risks are and then develop mitigating plans around that. What is your contingency plan if somebody gets in and shuts the system down? On our ships we do have engine failures, we do have to deal with them; this is not a hardware issue, it is a software issue. They should be treated as one and the same really.

Nigel Cleave
It is about education and training and is not just about starting with the IT department, it has to be taken seriously from the top and reviewing the real threats in your guidelines are exactly that Angus. The industry has to be aware and accept that the issue is real and increase this knowledge through education and training. Videotel is now in the process of producing a Cyber Security training course in conjunction with BIMCO. Training is vital for all aspects of seafaring and must be tested as an obvious step. The training has to go hand-in-hand with legislative change with seafarers having to buy into mitigating the threat too.

Denis Petropoulos
You can force your own management to have the guidelines onboard ship, but I still feel we have to look at what happens if there is a cyber attack. What is going to happen and how do we defend the ship? We haven't had crime in a container yard where people can walk into a container yard and crank open a container and see something sinister in the back of it. We have had people smuggling in drugs below the waterline of ships for instance. All these crimes are linked up for a purpose; the biggest problem in my view is the safety of the ship, crew and the cargo. Crew is paramount and we need to look at a way to handle that when the crime occurs. And then eliminate it and start again.

Peter Hinchliffe
The first stage is to make sure that the equipment you buy has an element of defence on it; the second stage is to make sure you have something that tells you there is a problem when you have a problem and the third stage is all about awareness. But I want to go on about the regulatory area, and there is clearly pressure for regulations to be developed but the argument that Angus is using is that regulation will not move quickly enough so that is why we are very much in favour of the guidelines approach, we can update these on a weekly basis and that is what is needed in order to respond to the threat out there. Any regulation only goes below the top surface of the problem, so we will end up with a regulation that is so out of date that is completely useless. So there should be some sort of indication in the ISM on what would be the best way forward so the attention of companies is drawn to this problem but to be prescriptive about regulation is not the right way to go about it.

Sean Moloney
Are the guidelines enough to keep Brussels and the regulators at bay?

Peter Hinchliffe
The stage where we are at the moment is that the guidelines are not enough because I think there is a mindset among regulators that it is something they can regulate but what are we trying to regulate here? Are we trying to regulate against cybercrime or are

we trying to put in place a regulatory mechanism that enables the industry to defend against it? We have got to be very clear about what the regulation sets out to be.

Rick Driscoll
The regulations will stay at a minimum level for a lot of the systems aboard the ship but this whole security issue is daunting and it is an ongoing process that has to be institutionalised in the organisations and it comes at a cost. So I think that is why some organisations aren't really stepping up to the plate right now but you have to look at the cost of the cyber incident against the cost of ongoing training for instance, scanning and assessments of your security stance but it will pay for itself. But there may have to be an incident or two before people realise.

Sean Moloney
For all of this to happen you have to have connectivity with a ship. And can connectivity to the ship be 100% secure?

Rick Driscoll
With connectivity in any environment – on land or at sea – there needs to be ongoing awareness, monitoring, training, and a plan to deal with cyber threats. Our professional services team works with fleet IT managers, onboard personnel, and others to design secure networks, normally separating crew and personal devices from operations networks, and blocking unknown inbound access. A key is to do cyber-threat training to ensure the crew understand threats to operations and their personal devices.

Sean Moloney
Does the industry really need to work together as a unit on this?

Angus Frew
The drawing of the guidelines was a combined effort with the industry with all members of the roundtable and IUMI (International Union of Maritime Insurance) so while BIMCO chose to lead on it, it was a joint effort. It is a living document.

Gerardo Borromeo
Unless we are aware of all of this we all become vulnerable points and there are enough vulnerable points on the ship. This is a way of life and we have to make it a way of life.

Katharina Stanzel
We have to shift our way of thinking because cyber does not equal IT because IT is just the vector; and a lot of the problems are similar to or parallel to issues we have already addressed in other areas, whether it is general vessel safety security systems so we have proper mechanisms in place, we just need to understand how the vectors work and that is more complicated because they are invisible because they are modern. All of us are dinosaurs and we don't understand how IT can work but once we have that understanding we can then apply the risk assessment tools we have used effectively elsewhere and we will be able to do that. To come back to the question about regulation, that is exactly the point; if regulation were to address the general principles it is probably already there, it is the IT aspect of it that it can never address because it is moving so fast.

Gerardo Borromeo
We are all vectors and potential carriers of the problem; it is a process issue.

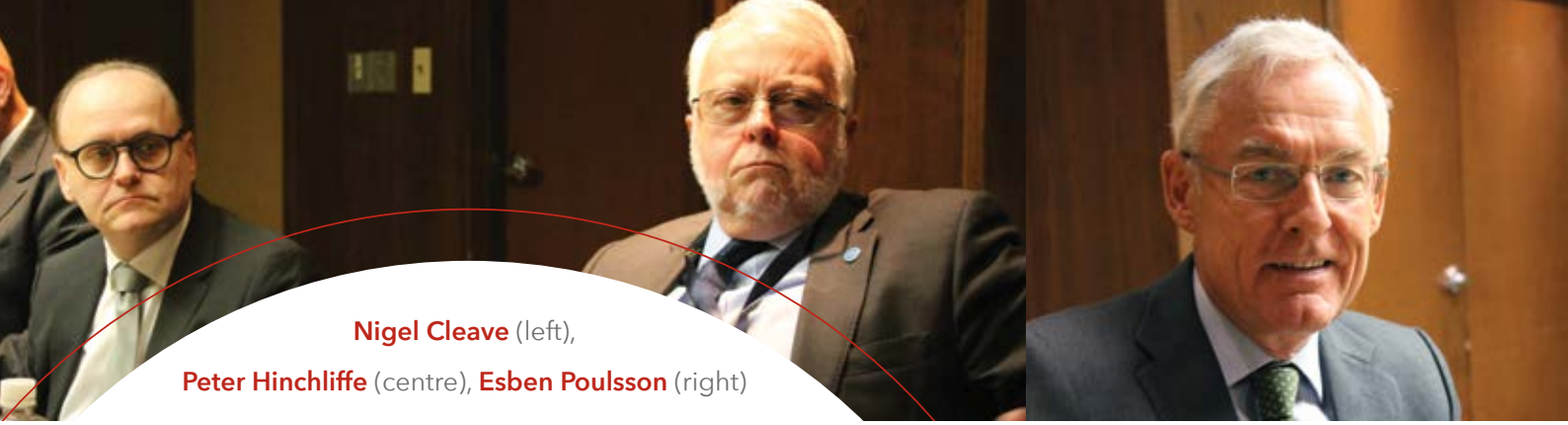
Angus Frew
I sometimes have to ring up my IT department because I have clicked on an attachment I shouldn't have, but the three organisations I have worked for have all have been attacked.

Denis Petropoulos
You have to ask yourself the question what are we fearful of? We are fearful of accidents, pollution, crew safety, so we have to target these hard points and work out how a cyber-attack is not going to be able to succeed. Why is the aviation industry having this type of conversation – because it doesn't want a plane to fall out of the sky.

Katharina Stanzel
For the fleets of my members, it is their biggest nightmare that something goes wrong with the ship, but I will come back to the process thinking; the processes are in fact a limited number like how would somebody get into the system, so I think we need to stay strategic enough to look at what the problems are and at least get a handle on it. I agree, the worst case or the Black Swan scenario that everyone is worried about, I wouldn't get scared into submission about that, we just have to systematically look at where are the ways in and out of the systems and how it could affect the steering of the ship, and once we have achieved that we can also then make the case to the regulator that we have thought of everything and we know how our systems work and all the components that could be affected and how they could be affected and this is the vector that could affect them. Once we have a handle on that I think we are in a good place. It doesn't mean that nothing is going to go wrong.

Denis Petropoulos
I agree with that.

Gerardo Borromeo
If we can create checkpoints or stop and think moments, this might be helpful. The challenge will be how do you create the checkpoints and stop and think moments that don't disrupt the difficult flow because so many things are happening at the same time. And break it down to the unit level or the individual. Even down to somebody who is viewed as a contractor element. Maybe this is where the investment needs to be made, certainly the more automated we become.



Nigel Cleave (left), **Peter Hinchliffe** (centre), **Esben Poulsson** (right)

Angus Frew
Because we see these little isolated units, called ships, that are not vulnerable onboard, we have to act in the same way as we act in the office; it has to be the same level of detail as how you set your systems up on the ship so you don't have your social systems on your control systems, and your control systems are on controlled networks. We audited a number of ships which helped us to get some data on this. As Peter said, there is a level of complacency that we need to drive out of the industry.

Rick Driscoll
It was mentioned that you want to bring the best practices from traditional industries to the ship, similar to you wanting to protect your ERP (Enterprise Resource Planning) system and then wanting to protect your navigation system, it is almost the same level of awareness.

Angus Frew
People are still being attacked onshore, and one of the vulnerabilities is the behaviour of people.

Nigel Cleave
And of course it's going to take a big incident and then everybody will be scrambling to try and fix it.

Sean Moloney
What can be done before and after a cyber-attack?

Viraj Nilakanta
Contingency plans; let's take for example the navigation system onboard, then say it gets hacked. Let's say you have two independent ECDIS but they have both failed - that is a worst-case scenario. So what is your contingency plan to navigate the paperless ship without ECDIS and without charts? Within our managed fleet we have about 160 ships that are paperless, but we do have contingency measures. What happens if ECDIS fails? Regulations are mandated to have two independent systems, but it is the same software that you are putting in both of the systems to update them. You uploaded one ECDIS to upgrade the software and then you load it in the other ECDIS. There is a virus in one which will be transferred into the other one. So it is about having contingency measures, you do drills. In our company we have drills every few months, where we turn off the ECDIS in the middle of the sea to see how they navigate. We have what we call "take me home charts", so before the voyage starts you have a plan for what happens if the ECDIS fails.

Gerardo Borromeo
The fact that cyber-attacks can compromise us means we should make this now part of our contingency plans onboard ship. Scale up the level of sophistication on the discussions, and it is an evolving thing and we have discussions here today. If there is a group of trade associations who continue to think ahead they can help the industry be more self-regulating, and that is very important because we can move much more rapidly than the regulators. We should continue to raise the level of sophistication in our thinking. There are disruptive elements out there and it is interesting that as the world gets smaller you think it would get easier but it is actually getting more complex. So the level of complexity in our thinking must continue to evolve and the speed at which the complex thinking comes up is the best way to stay ahead of the game.

Nigel Cleave
Training and a corporate policy are essential prerequisites but how many companies, for instance, have a cybercrime action plan? Are there file back-up systems in place, can elements of the system be safely shut down? How quickly can a ship/company be back up and running? I am sure that offices are invariably far more protected today than vessels.

Katharina Stanzel
As a merchant marine industry we are still training our young officers to use the tools they need when the ECDIS fails, while some navies and coastguards took it out of their curriculum. And they are now going back to sextant training and bringing it back in because of this reason. We have never, as an industry, taken it out.

Peter Hinchliffe
Viraj has raised an interesting point because the ECDIS regulation which stipulates having two independent systems was written in such a way that they should be, if there was a physical failure, completely independent. But now we need to go back and have another look at that regulation because maybe the one safeguard is if you do an upgrade in one, let it run for a week before you do an upgrade in the other.

Sean Moloney
Thank you very much lady and gentlemen. ●