**Future Thinking S3 E4: Securing the Future: Cyber Threats in Shipping**

00:00:03.980 --> 00:00:11.520
<v SPEAKER_2>Hello, and welcome to Future Thinking, an Alongside mini-series from NorthStandard, one of the world's leading marine insurers.

00:00:11.520 --> 00:00:21.600
<v SPEAKER_2>I'm Helen Barden, and in this mini-series, we will look at the advances in technology and the opportunities and challenges this brings to the maritime industry.

00:00:21.600 --> 00:00:31.280
<v SPEAKER_2>In this episode, I'm joined by Kimberly Tam of the Alan Turing Institute, and we will be delving into the world of AI with particular focus on cyber security.

00:00:32.900 --> 00:00:37.360
<v SPEAKER_2>I'm delighted you could join me today, Kimberly, and welcome to the Alongside podcast.

00:00:37.360 --> 00:00:37.560
<v SPEAKER_1>Thanks.

00:00:37.560 --> 00:00:38.980
<v SPEAKER_1>It's great to be here.

00:00:38.980 --> 00:00:57.020
<v SPEAKER_2>Before going into the role of AI and cyber security, perhaps we could start by you giving your view on how prevalent you think cyber attacks are in the shipping industry, and perhaps what type of cyber attack tends to hit the shipping industry most.

00:00:57.480 --> 00:01:16.660
<v SPEAKER_1>So, from our reports and also from other people's reports, like the US Coast Guard and companies that track threats in the maritime sector, we've been seeing a huge increase in pretty basic things like phishing attacks, so attacks that go to your email, trying to fool you into clicking on a link.

00:01:16.660 --> 00:01:24.560
<v SPEAKER_1>We've also seen an increase in ransomware, so that is when people take away your access to your data and hold that for ransom.

00:01:25.040 --> 00:01:35.420
<v SPEAKER_1>That can go in two different ways, they can hold your data for ransom, so you can't access it, and they can also demand a ransom so that they don't release your data to the public.

00:01:35.420 --> 00:01:39.200
<v SPEAKER_2>Do you think those attacks are increasing as well?

00:01:40.240 --> 00:01:44.480
<v SPEAKER_2>The chances of them happening now are more this year than last year?

00:01:44.480 --> 00:01:45.000
<v SPEAKER_1>Yeah.

00:01:45.000 --> 00:01:47.380
<v SPEAKER_1>We've been seeing pretty steady increases.

00:01:47.380 --> 00:01:51.200
<v SPEAKER_1>It's hard to know exactly how many cyber attacks are happening out there.

00:01:51.200 --> 00:01:56.520
<v SPEAKER_1>One of the problems that we are facing is that reporting is not always accurate.

00:01:56.520 --> 00:02:03.560
<v SPEAKER_1>Sometimes things get mislabeled as a human error or a more of a technical issue.

00:02:03.560 --> 00:02:09.100
<v SPEAKER_1>And also digital forensics is not as strong in the sector as something like the IT sector.

00:02:09.100 --> 00:02:12.020
<v SPEAKER_1>So there's probably a lot of attacks happening that we don't know of.

00:02:12.020 --> 00:02:16.660
<v SPEAKER_1>But the ones we do know of is definitely ticking up for the last few years.

00:02:16.660 --> 00:02:28.760
<v SPEAKER_2>So it's definitely something that we should be taking very seriously then, if it's going to be something that becomes kind of an increasing threat to the maritime industry by the sounds of things.

00:02:28.760 --> 00:02:43.880
<v SPEAKER_2>So in terms of your role at the Alan Turing Institute and the focus around AI and the role in cyberattacks, what role does AI play in actually detecting or stopping cyberattacks?

00:02:43.880 --> 00:02:49.060
<v SPEAKER_1>Yeah, so in terms of using AI on the defense side, there's several aspects to it.

00:02:49.060 --> 00:02:53.340
<v SPEAKER_1>So one difficult thing about cyberattacks is they can happen 24-7.

00:02:53.600 --> 00:02:56.340
<v SPEAKER_1>It's not like there's a time of day when they tend to happen.

00:02:56.340 --> 00:03:04.760
<v SPEAKER_1>And burnout amongst cyber incident responders is actually pretty high because there are people trying to fight digital attacks that could happen whenever.

00:03:04.760 --> 00:03:06.720
<v SPEAKER_1>And also, there's a huge quantity of them.

00:03:06.720 --> 00:03:13.680
<v SPEAKER_1>The way that phishing emails happen, you can send out mass amounts of campaigns and just see what comes back.

00:03:13.680 --> 00:03:18.780
<v SPEAKER_1>So it's very difficult for people to combat these kind of threats.

00:03:19.140 --> 00:03:26.420
<v SPEAKER_1>So one of the places that we're looking to use AI is to help take away some of the menial tasks, some of the burdens.

00:03:26.420 --> 00:03:31.640
<v SPEAKER_1>So help filter some of the alerts, help look for threats on the network.

00:03:31.640 --> 00:03:37.360
<v SPEAKER_1>So tools to help existing cybersecurity experts deal with the load better.

00:03:37.360 --> 00:03:38.620
<v SPEAKER_1>That's one level.

00:03:38.620 --> 00:03:44.240
<v SPEAKER_1>The next level is actually starting to create more intelligent AI to do a lot of this themselves.

00:03:44.240 --> 00:03:59.920
<v SPEAKER_1>At the moment, we do need a human analyst involved, but there is discussions of intelligent firewalls, so AI to understand the context of an attack, because some things that would be okay in some circumstances is not okay in others.

00:03:59.920 --> 00:04:03.660
<v SPEAKER_1>So it's really hard to just blanket say no or blanket say yes.

00:04:03.660 --> 00:04:10.980
<v SPEAKER_1>So the more intelligent AI can be, the better it will be to defend without human interaction.

00:04:10.980 --> 00:04:12.120
<v SPEAKER_2>That's really interesting.

00:04:12.300 --> 00:04:23.860
<v SPEAKER_2>And I think it's, I mean, I see phishing emails coming in to my inbox sometimes, and actually it is very difficult to know whether it's a genuine email or not.

00:04:23.860 --> 00:04:31.620
<v SPEAKER_2>So if there's AI that can actually help you make that decision, then I can imagine that's a very useful tool.

00:04:31.620 --> 00:04:37.220
<v SPEAKER_2>How vulnerable is AI itself to cyber attacks?

00:04:37.220 --> 00:04:44.600
<v SPEAKER_1>So when we talk about the vulnerabilities of AI, one of the things that we talked with NCSE about is the life cycle of AI.

00:04:44.600 --> 00:04:52.240

<v SPEAKER_1>So kind of when AI is being created, when it's actually developed and being used, so there's different stages of the life cycle of AI.

00:04:52.240 --> 00:04:54.760
<v SPEAKER_1>So there's vulnerabilities at each stage.

00:04:54.760 --> 00:05:00.500
<v SPEAKER_1>So one of the things that we think more at the beginning is the AI is only as good as the data you train on it.

00:05:00.500 --> 00:05:06.140
<v SPEAKER_1>So the earliest thing you can do is poison or manipulate the data that is being used to train these AI.

00:05:06.620 --> 00:05:09.900
<v SPEAKER_1>It could create blind spots, it could make it ineffectual.

00:05:09.900 --> 00:05:19.880
<v SPEAKER_1>So the earliest attacks that we've seen is actually not attacking the AI itself, but attacking the data and the sensors or whatever makes that data to feed into the AI.

00:05:19.880 --> 00:05:26.500
<v SPEAKER_1>The second stage of AI is when you attack the AI itself where it's stored in the computer.

00:05:26.500 --> 00:05:37.080
<v SPEAKER_1>So one of the things that we've seen is people can actually go in and find the files associated with a trained AI, chained variables, and again, that can create blind spots and weaknesses.

00:05:37.080 --> 00:05:41.500
<v SPEAKER_1>There are a few attacks that you might see after the AI has been developed.

00:05:41.500 --> 00:05:55.900
<v SPEAKER_1>So when it's out there doing its thing, probably one of the most famous visible examples are when people were not happy with facial recognition, so they painted symbols on their faces and the AI could no longer function and see that.

00:05:55.900 --> 00:06:02.720
<v SPEAKER_1>So those are the three stages, I think, that AI can be vulnerable to kind of digital attacks.

00:06:02.720 --> 00:06:10.640
<v SPEAKER_2>And in the maritime industry, which parts of the industry are more vulnerable to cyber attacks?

00:06:10.640 --> 00:06:13.880
<v SPEAKER_2>So are we talking about the ships themselves?

00:06:13.880 --> 00:06:17.660
<v SPEAKER_2>Are we talking about the onshore infrastructure?

00:06:17.660 --> 00:06:22.900
<v SPEAKER_2>I know that you do work particularly in relation to the offshore industry as well.

00:06:22.900 --> 00:06:26.580
<v SPEAKER_2>Which areas are most at risk of cyber attacks?

00:06:26.720 --> 00:06:33.320
<v SPEAKER_1>That's a really hard question to ask, because I think, especially for me and with my background, everything is vulnerable.

00:06:33.320 --> 00:06:35.480
<v SPEAKER_1>They're just vulnerable in different ways.

00:06:35.480 --> 00:06:44.800
<v SPEAKER_1>And I think another critical aspect is whenever we talk to people about risk, it's not just, are they vulnerable, but is someone potentially going to exploit it?

00:06:44.800 --> 00:06:50.560
<v SPEAKER_1>Because a lot of systems are vulnerable, but no one cares to exploit it because they get nothing out of it.

00:06:50.560 --> 00:06:59.640
<v SPEAKER_1>So it's that mix of, there's a lot of vulnerabilities, I think, in all technology, not just across the maritime sector, like you say, port ships and things like that.

00:06:59.640 --> 00:07:01.720
<v SPEAKER_1>They all have different types of vulnerabilities.

00:07:01.720 --> 00:07:12.920
<v SPEAKER_1>So legacy systems is mentioned a lot for kind of older ships, but also constant connectivity is a vulnerability that we mention a lot in newer ships.

00:07:12.920 --> 00:07:13.880
<v SPEAKER_1>Same thing with ports.

00:07:13.880 --> 00:07:24.340
<v SPEAKER_1>So it's different vulnerabilities for different parts of the sector, but it's also understanding which ones could lead to bad impact and which ones are just kind of inherent to digitization.

00:07:24.700 --> 00:07:28.520
<v SPEAKER_1>And but will have little impact and so kind of can be left alone.

00:07:28.760 --> 00:07:46.160
<v SPEAKER_2>And do you do modeling around these different risks then, whether it's in relation to risks affecting ships or the onshore infrastructure, and kind of test where those vulnerabilities might most likely be exploited?

00:07:46.160 --> 00:07:47.800
<v SPEAKER_1>Yeah, so we do both.

00:07:47.800 --> 00:07:52.800
<v SPEAKER_1>We do lots of kind of ground truth testing to see whether or not a vulnerability exists.

00:07:53.420 --> 00:08:03.600
<v SPEAKER_1>So this is a little bit more in the University of Plymouth side of things, but we often get equipment that we can test to see what are the actual vulnerabilities and not theorize it.

00:08:03.600 --> 00:08:15.720
<v SPEAKER_1>But a lot of that then can feed into the risk assessment, which you were kind of mentioning, is how do we kind of prioritize these issues and which ones have the biggest impact and use that information to kind of move forward.

00:08:16.400 --> 00:08:23.760
<v SPEAKER_2>And what are the cost impacts usually associated with cyber attacks then?

00:08:23.760 --> 00:08:36.040
<v SPEAKER_2>Obviously, there's the risk of the cyber attack happening, but actually what kind of figures are we talking in terms of the potential losses to the industry when it comes to cyber attacks?

00:08:36.040 --> 00:08:47.280
<v SPEAKER_1>Because of the way we haven't been able to identify all cyber attacks happening in the sector, the ones we typically know about are the ones that stop operations, you know, ransomware, things like that.

00:08:47.280 --> 00:08:54.320
<v SPEAKER_1>So when that happens, we can often calculate the cost of an incident based on the disturbance.

00:08:54.320 --> 00:09:02.360
<v SPEAKER_1>So how long was the port shut down, which parts of the port, you know, how long it takes to get further infrastructure to come back online.

00:09:02.360 --> 00:09:14.300
<v SPEAKER_1>And that's been interesting because people in the maritime sector usually can ballpark the cost of it pretty well because they understand that the sector is very interconnected, shipping is very interconnected.

00:09:14.980 --> 00:09:21.680
<v SPEAKER_1>But actually, when we talk to the public about risk perception around this, their numbers are totally off.

00:09:21.680 --> 00:09:30.140
<v SPEAKER_1>I actually went to do a talk in Austria and asked them what they think a cyber attack would cost them if there was one in the port of Alenthia.

00:09:30.140 --> 00:09:31.740
<v SPEAKER_1>This was tied to another project.

00:09:31.740 --> 00:09:34.140
<v SPEAKER_1>And they said, we're a landlocked country.

00:09:34.140 --> 00:09:36.480
<v SPEAKER_1>What happens out there doesn't matter to us.

00:09:36.480 --> 00:09:40.580
<v SPEAKER_1>And then I showed them the costs based on, you know, the supply chain, all these things.

00:09:40.580 --> 00:09:41.580
<v SPEAKER_1>And they were surprised.

00:09:41.780 --> 00:09:47.020
<v SPEAKER_1>So it's really interesting to see that disconnect between people who work in this industry and people who don't.

00:09:47.020 --> 00:09:57.540
<v SPEAKER_2>Yeah, I mean, the point you make there about the fact that it's not just going to be the physical port itself that ends up with the vulnerability and the cost exposure.

00:09:57.540 --> 00:10:00.040
<v SPEAKER_2>But actually, you do need to look at the full supply chain.

00:10:00.260 --> 00:10:12.200
<v SPEAKER_2>And that's a very broad spectrum of stakeholders that need to be concerned about this and also need to be, I guess, engaging in protecting their systems.

00:10:12.200 --> 00:10:22.300
<v SPEAKER_2>How likely are, I suppose, findings from real world testing and case studies shared?

00:10:22.560 --> 00:10:30.840
<v SPEAKER_2>How are they used in terms of actually improving the cyber resilience of the maritime industry?

00:10:30.840 --> 00:10:47.060
<v SPEAKER_1>So if a vulnerability we see or find or it's been reported to us is specific to one manufacturer or something like that, we tend to just go to them directly, let them know what's happened, and then if they're up for it, we'll let them know how to fix it.

00:10:47.060 --> 00:10:54.540
<v SPEAKER_1>If we start seeing a pattern, so for example, there's a lot of SMEs building autonomy around my area.

00:10:54.540 --> 00:11:02.300
<v SPEAKER_1>So if there's a common vulnerability that we see across a lot of SMEs, we might do something a bit more global, a workshop.

00:11:02.300 --> 00:11:06.600
<v SPEAKER_1>We've been doing more and more kind of going up to policy and regulation.

00:11:06.600 --> 00:11:12.560
<v SPEAKER_1>So I was at MSC 109 for mass regulations, I think it was a week ago.

00:11:12.560 --> 00:11:17.840
<v SPEAKER_1>So there's a lot more pushing it up into regulation and policy as well.

00:11:17.840 --> 00:11:19.960
<v SPEAKER_1>And then there's also a lot of training.

00:11:19.960 --> 00:11:29.420
<v SPEAKER_1>So we do cybersecurity, maritime cybersecurity training for students, people who are working in industry and just want to refresher.

00:11:29.420 --> 00:11:32.760
<v SPEAKER_1>So we try and disseminate as many ways as possible.

00:11:32.760 --> 00:11:47.880
<v SPEAKER_2>So just picking up on the need for training when it comes to cybersecurity, how important are we as humans then, when it comes to detecting possible cyber attacks and vulnerabilities?

00:11:47.880 --> 00:11:49.740
<v SPEAKER_1>I think very important.

00:11:49.740 --> 00:12:03.020
<v SPEAKER_1>I think human AI teaming, or how all the other terms are really important, because AI is vulnerable to other AI and computing things.

00:12:03.020 --> 00:12:13.380
<v SPEAKER_1>So having different types of thinking process is useful for that extra security, because the things that humans will spot are things that difficult for computer spot.

00:12:13.380 --> 00:12:18.940
<v SPEAKER_1>And the same reason why we use AI for so much, because it's good at spotting patterns that humans are very good at.

00:12:18.940 --> 00:12:26.200
<v SPEAKER_1>So having the two together teamed up, I think, could be a very powerful tool for detecting cyber attacks and other things.

00:12:26.200 --> 00:12:37.020
<v SPEAKER_2>And do you think that the human intervention will, I guess, continue to be required when it comes to identifying cyber attacks?

00:12:37.020 --> 00:12:43.240
<v SPEAKER_2>AI is not going to get so clever that actually we don't need to think about it.

00:12:43.240 --> 00:12:47.160
<v SPEAKER_1>Not in the short term, as far as I can tell.

00:12:47.540 --> 00:12:55.980
<v SPEAKER_1>The amount of work that is necessary to get an AI to that level to replace a human in that aspect, I think, is already difficult.

00:12:55.980 --> 00:12:59.780
<v SPEAKER_1>And then, as we've talked, AI is not full proof.

00:12:59.780 --> 00:13:02.000
<v SPEAKER_1>It is susceptible to cyber attacks.

00:13:02.000 --> 00:13:08.420
<v SPEAKER_1>So building an AI to detect cyber attacks that could be vulnerable to cyber attacks doesn't really solve the problem.

00:13:08.420 --> 00:13:14.840
<v SPEAKER_1>So I do think we need multiple layers of defense, AI, people, other framework, things like that.

00:13:15.460 --> 00:13:18.440
<v SPEAKER_1>So I don't think it's going to be soon.

00:13:18.440 --> 00:13:26.060
<v SPEAKER_2>How much information is likely to be shared or useful across the industry?

00:13:26.060 --> 00:13:43.500
<v SPEAKER_2>So obviously, if there's a, I guess, an individual vessel issue, it might be that actually what has happened with that vessel could, in theory, be replicated across other vessels, whether that's within the same fleet or whether that's within another ship owners fleet of ships.

00:13:44.180 --> 00:13:58.480
<v SPEAKER_2>Do you see there being any more dialogue and openness around cyber attacks and the risks, and trying to improve the resilience of the industry by sharing that information?

00:13:58.480 --> 00:14:02.820
<v SPEAKER_1>Yeah, I think information sharing is a huge topic at the moment.

00:14:02.820 --> 00:14:11.280
<v SPEAKER_1>There's a lot of discussion on how people are worried about damage to reputation or leaking something and showing people that they have been vulnerable.

00:14:11.460 --> 00:14:19.740
<v SPEAKER_1>But in all other sectors, the studies have shown that the more information you share, the better you are, the more secure you are.

00:14:19.740 --> 00:14:31.820
<v SPEAKER_1>So one of the big things and one of the things that highlights why maritime cybersecurity is different from just kind of office, IT cybersecurity, is that it could be as a result of something in the location.

00:14:31.820 --> 00:14:40.320
<v SPEAKER_1>So something like jamming is very regional, whereas something like a spam mass campaign usually is aimed towards a company.

00:14:41.000 --> 00:14:52.240

<v SPEAKER_1>And wherever those vessels or people may be, so knowing, communicating, knowing what is going on to not just yourself, but people around you can help you understand what type of attack is happening.

00:14:52.240 --> 00:14:56.500
<v SPEAKER_1>And that's kind of the critical part to then preventing or mitigating that attack.

00:14:56.500 --> 00:15:25.580
<v SPEAKER_2>Yeah, and I think the mitigation point you make there is obviously really important, because actually, if you think of a busy port and how many vessels there are operating within ports, if there is vulnerability with one of those ships, actually that could cause considerable damage potentially, depending on the cyber attack to the port infrastructure as well, so that the need to share information where it is possible to try and mitigate those risks and those losses is vital really.

00:15:25.580 --> 00:15:38.660
<v SPEAKER_2>Just kind of circling back to the point you made about mass and the fact that you were attending the MSC meeting looking at the safety of autonomous vessels.

00:15:38.660 --> 00:15:43.500
<v SPEAKER_2>How do you address cyber security in that context?

00:15:43.500 --> 00:15:50.380
<v SPEAKER_2>So is that looking at, you mentioned obviously earlier, the areas where AI itself can be vulnerable.

00:15:50.380 --> 00:15:53.580
<v SPEAKER_2>So is that a similar approach in terms of autonomous vessels?

00:15:53.580 --> 00:16:09.220
<v SPEAKER_2>You have to kind of look at those different areas, looking at the data, looking at the AI and looking at actually how it gets used once it's implemented, to ensure that it's as resilient as possible to cyber attacks.

00:16:09.220 --> 00:16:11.520
<v SPEAKER_2>It would be really interesting to hear your take on that.

00:16:11.520 --> 00:16:13.560
<v SPEAKER_1>Yeah, it was interesting.

00:16:13.560 --> 00:16:24.720
<v SPEAKER_1>And like you said, AI was mentioned, but in terms of what actually got onto paper, I think it was kind of lumped into more software.

00:16:24.900 --> 00:16:32.520
<v SPEAKER_1>So as an aspect of general software, AI, but I suppose ML and machine learning and things like that would also get lumped in.

00:16:32.520 --> 00:16:36.920
<v SPEAKER_1>So it is addressed, although it tends to be under bigger umbrella terms.

00:16:36.920 --> 00:16:39.880

<v SPEAKER_1>And cyber attacks is interesting as well.

00:16:39.880 --> 00:16:44.680
<v SPEAKER_1>One of the things I pointed at was cyber attack kind of implies an attacker.

00:16:44.680 --> 00:16:48.960
<v SPEAKER_1>So a possible broader term would be something like cyber incident.

00:16:48.960 --> 00:16:59.120
<v SPEAKER_1>You don't know exactly whether it was intentional, non-intentional, error, AI, person, but you do know that there was an incident evolving kind of a cyber trigger.

00:16:59.120 --> 00:17:04.100
<v SPEAKER_1>So being able to discuss that has been really useful, both from the software side.

00:17:04.100 --> 00:17:06.160
<v SPEAKER_1>The other thing that was mentioned a lot was connectivity.

00:17:06.160 --> 00:17:12.500
<v SPEAKER_1>So I think they're very interested in kind of the cyber attacks from external parties and not kind of internally.

00:17:12.500 --> 00:17:33.040
<v SPEAKER_2>And in terms of the connectivity side of things, if you have data that is just going out from a vessel, is that still a cyber risk in terms of the vessel itself, or because you've just got the data effectively, say coming off sensors from a vessel, does the risk not arise?

00:17:33.040 --> 00:17:34.500
<v SPEAKER_1>It's an interesting question.

00:17:34.500 --> 00:17:44.300
<v SPEAKER_1>So if it's just a one-way transmission of data, that does reduce a lot of vulnerabilities because nothing's coming back.

00:17:44.300 --> 00:17:48.600
<v SPEAKER_1>However, it's very hard to enforce a one-way channel.

00:17:48.760 --> 00:17:50.780
<v SPEAKER_1>So you can do that with physical wires.

00:17:50.780 --> 00:17:57.660
<v SPEAKER_1>But when it comes to satellite communication, often the communication channel is still two directions.

00:17:57.660 --> 00:17:59.320
<v SPEAKER_1>You only just use one.

00:17:59.320 --> 00:18:08.820
<v SPEAKER_1>So if that channel is there, sometimes an attacker could still find a way to enable the other direction of communication into the vessel.

00:18:08.820 --> 00:18:13.580
<v SPEAKER_1>So it's an interesting question of what's possible versus what's not.

00:18:13.620 --> 00:18:29.840
<v SPEAKER_2>That's really interesting because it's like I say earlier in the decarbonization space when you're thinking about data coming off ships to try and improve efficiency or understand how the vessels operating, and to be able to change orders.

00:18:29.840 --> 00:18:40.780
<v SPEAKER_2>You're generally thinking of the data coming off the ship rather than it being two-way and therefore, I guess, an understanding of perhaps reduced risk of cyber incidents.

00:18:41.020 --> 00:18:51.420
<v SPEAKER_2>And I suppose as well, it's important to understand the sensitivity of the data itself when you're assessing the concerns around the cyber risk as well.

00:18:51.420 --> 00:19:06.200
<v SPEAKER_2>Before we finish, I just wonder if you have any, I guess, top tips when it comes to ensuring good cyber awareness within companies, having good procedures in place?

00:19:06.200 --> 00:19:16.320
<v SPEAKER_1>I think the biggest benefit we've seen to people improving their cybersecurity posture across the organizations we've talked to is communication between silos.

00:19:16.320 --> 00:19:20.480
<v SPEAKER_1>So you mentioned ports and like a busy port with lots of ships in it.

00:19:20.480 --> 00:19:29.860
<v SPEAKER_1>One of the things we've highlighted with some of our previous research is that even if a port is completely secure, you've got ships coming in and out, people coming in and out, and all of that has technology.

00:19:29.860 --> 00:19:33.180
<v SPEAKER_1>So their security could affect yours.

00:19:33.340 --> 00:19:36.300
<v SPEAKER_1>In cybersecurity, we talk a lot about the weakest link.

00:19:36.300 --> 00:19:41.520
<v SPEAKER_1>So even though your stuff is good, you could still be negatively impacted by everyone else.

00:19:41.520 --> 00:19:44.440
<v SPEAKER_1>So it's getting people to talk to each other.

00:19:44.440 --> 00:19:54.940
<v SPEAKER_1>So another random interaction we've started doing is wind farms and autonomy, because those two are likely to interact a lot with each other, and that could lead to vulnerabilities.

00:19:54.940 --> 00:20:00.160
<v SPEAKER_1>So it's breaking down the silos, both across the sector, but also up and down.

00:20:00.160 --> 00:20:14.860
<v SPEAKER_1>So getting the people who work on the ground to talk to the higher ups, talk about what they've seen, because I think also a lot of cyber incidences don't fully make, the reports don't fully make it to the top at the moment.

00:20:14.860 --> 00:20:22.260
<v SPEAKER_1>So I think there's a lot of discussion to be had to break down the silos and kind of trade information, which I think we talked about a lot.

00:20:22.260 --> 00:20:37.020
<v SPEAKER_2>That's really helpful, and it raises an interesting point around actually having some more transparency and openness around these issues to try and improve the resilience of the industry.

00:20:37.120 --> 00:20:50.640
<v SPEAKER_2>And it's not just, you know, the fact that you can't just be comfortable that you, as an individual company, have got all of your cyber ducks in a row, if you like, actually, you do need to look at the bigger picture.

00:20:50.640 --> 00:20:53.360
<v SPEAKER_2>Thank you very much for that brilliant insight today, Kimberly.

00:20:53.360 --> 00:20:55.800
<v SPEAKER_2>It's been great to have you on the podcast.

00:20:55.800 --> 00:20:56.260
<v SPEAKER_1>Thank you.

00:20:56.260 --> 00:20:58.320
<v SPEAKER_1>And it was great to be here.

00:20:58.320 --> 00:21:04.700
<v SPEAKER_2>Remember to listen to other episodes in this miniseries where we look at the impact of new technology on the maritime industry.

00:21:05.300 --> 00:21:13.820
<v SPEAKER_2>You'll find the Alongside podcast and this miniseries on the NorthStandard website at northstandard.com or wherever you get your podcasts.

00:21:13.820 --> 00:21:17.100
<v SPEAKER_2>You can also click follow to ensure you don't miss an episode.

00:21:17.100 --> 00:21:20.120
<v SPEAKER_2>So from me, Helen Barden, thank you for listening and bye for now.