CRA: Are You Ready for September 2026? - Webinar Transcript

1
00:00:05.520 --> 00:00:07.309
Pepijn van der Laan: Cool. Awesome.

2
00:00:08.770 --> 00:00:15.529
Pepijn van der Laan: Nice day for a webinar. We see the counter of people coming in.

3
00:00:15.680 --> 00:00:23.590
Pepijn van der Laan: Increasing, so let's give that a moment until it… More or less stabilizes.

4
00:00:29.860 --> 00:00:31.370
Pepijn van der Laan: Perfect.

5
00:00:31.690 --> 00:00:33.690
Pepijn van der Laan: Already a good crowd.

6
00:00:34.700 --> 00:00:41.650
Pepijn van der Laan: Over the hundreds participants already in the meeting. That is great. Welcome to everyone.

7
00:00:45.210 --> 00:00:52.120
Pepijn van der Laan: So… Maybe slowly but surely, we can start the…

8
00:00:52.180 --> 00:01:06.140
Pepijn van der Laan: start the webinar now. Quite some people have joined us. There are still some people jumping in a bit later, but they're, of course, just as welcome as the early joiners.

9
00:01:06.140 --> 00:01:12.670
Pepijn van der Laan: So, welcome to our Get Ready for September 11th webinar.

10
00:01:12.700 --> 00:01:13.840
Pepijn van der Laan: So.

11
00:01:13.950 --> 00:01:28.459
Pepijn van der Laan: just to make sure, this is about the CRA, the Cyber Resilience Act, which, is the European regulation for… for cyber security, so if you have other associations with September 11,

12
00:01:29.490 --> 00:01:38.180
Pepijn van der Laan: apology for any confusion. But this is really about the the EU, the EU regulation on cybersecurity. So

13
00:01:38.320 --> 00:01:52.830
Pepijn van der Laan: before we dive into the content, let us first introduce ourselves as your host for today. So, I'm Pep, I'm the Technical Director at Memco Digital.

14
00:01:53.140 --> 00:02:03.330
Pepijn van der Laan: long experience in scaling AI, in strategic advisory, in building capabilities of technical teams and growing digital trust.

15

00:02:03.330 --> 00:02:22.820
Pepijn van der Laan: Really for a long time working on AI, on security related questions, questions around the implementation at scale of, yeah, of large technological systems. So happy to be here today also together with.

16
00:02:22.820 --> 00:02:27.200
Pepijn van der Laan: With Gustavo. Gustavo, if you could briefly introduce yourself, that would be awesome.

17
00:02:27.830 --> 00:02:40.310
Gustavo Sanchez: Yes, thank you, Pep. My name is Gustavo. I focus on the trustworthy AI as a consultant within Nemko Digital, also working within cybersecurity topics.

18
00:02:40.330 --> 00:02:56.869
Gustavo Sanchez: For example, regulatory compliance in the CRA, and my background is on software engineering, and I have done research for quite a few years, and I obtained a PhD on the intersection of AI and cybersecurity.

19
00:02:57.360 --> 00:03:05.070
Gustavo Sanchez: And now in this presentation, I will be diving deeper on the reporting obligations.

20
00:03:06.550 --> 00:03:21.609
Pepijn van der Laan: Yes, perfect. So, thanks a lot, Gustavo, great to have you. This is your first, Nemko webinar, so, that is a great, that's a great start, good topic to start on. So, today, what will we be talking about?

21
00:03:21.610 --> 00:03:40.780
Pepijn van der Laan: Briefly introducing, Nemko Digital for those for whom it's necessary, for those, who have been in more of our webinars, apologies for the

repetition. It's always good to, to know who's there. From there, we'll dive into a brief recap.

22
00:03:40.780 --> 00:03:47.589
Pepijn van der Laan: of the Cyber Resilience Act to give you an overview. What was this about again? What is the

23
00:03:47.590 --> 00:03:56.679
Pepijn van der Laan: And what is this that is coming at you, including the various deadlines that there are for the Cyber Resilience Act?

24
00:03:56.700 --> 00:04:12.370
Pepijn van der Laan: After that, we'll dive into the first, the first, the first deadline that there is, which is, September 11th of, 20, 2026. So this year, only, only three months, out,

25
00:04:12.630 --> 00:04:15.659
Pepijn van der Laan: Or 2 months even, where…

26
00:04:15.810 --> 00:04:34.779
Pepijn van der Laan: the first obligations around reporting already kick in. We'll talk a bit about, yeah, how do you get started if you are not yet on the path towards compliance, and then open the floor also to questions from the participants.

27
00:04:36.270 --> 00:04:41.349
Pepijn van der Laan: So with that, yeah, let me first briefly introduce Nympho Digital.

28
00:04:41.700 --> 00:04:48.830
Pepijn van der Laan: So, Namco Digital, part of Namco Group, focus on the

29
00:04:48.960 --> 00:04:56.890
Pepijn van der Laan: the digital side of, of compliance and, and product. Of course,

30
00:04:57.130 --> 00:05:09.869
Pepijn van der Laan: from our, center in, in Amsterdam, where we have our global center of excellence, we basically serve, clients around, around the globe,

31
00:05:10.510 --> 00:05:34.789
Pepijn van der Laan: The way we support is typically compared to traditional Nemko a bit more advisory also because in the digital space there's so much going on and so much evolving that in the balance between the traditional TIC testing inspection certification and advisory as Nemko Digital within Nemko Group we focus a bit more on that on that advisory side.

32
00:05:34.830 --> 00:05:48.230
Pepijn van der Laan: of course, closely working together with our colleagues, in Norway and other countries, who perform more the, that testing inspection certification side of the, of the business. And together.

33
00:05:48.500 --> 00:05:53.250
Pepijn van der Laan: And we help we help companies to come towards conformance. So.

34
00:05:53.750 --> 00:06:17.679
Pepijn van der Laan: From an EMCO Digital perspective, where is our focus in terms of the projects we're working on, the issues that we support our clients with? Of course, there's regulatory compliance. Yes, a lot of that is about AI and the AI Act, but also other regulations like today, the Cyber Resilience Act is what we help clients on that journey towards compliance.

35

00:06:17.680 --> 00:06:26.390
Pepijn van der Laan: conformity, but not only regulatory compliance, also standards like ISO, in particular ISO 42000.

36
00:06:26.390 --> 00:06:30.559
Pepijn van der Laan: Is something that we, yeah, that we provide services on.

37
00:06:30.560 --> 00:06:46.409
Pepijn van der Laan: as well as, global market access. And when it comes to AI, we also do have our own, Namco AI Trustmark, as a proprietary, scheme for, for certifying AI, AI systems,

38
00:06:46.780 --> 00:06:59.410
Pepijn van der Laan: from those more, regulatory and compliance-focused, elements, yeah, we also step into what is more the, I would say, the…

39
00:06:59.600 --> 00:07:18.880
Pepijn van der Laan: General advisory and that can be around technical assurance and AI testing, but also about tool implementations around assurance and around governance maturity as well as strategy and roadmap type work.

40
00:07:18.880 --> 00:07:32.530
Pepijn van der Laan: where we, where we also support. So, a broad, range of, of services. Today, we'll really focus, focus on one, regulation in particular, the Cyber Resilience Act,

41
00:07:32.750 --> 00:07:42.340
Pepijn van der Laan: and dive into the concrete obligations also towards September 11th later this year.

42

00:07:42.480 --> 00:07:43.510
Pepijn van der Laan: So…

43
00:07:43.890 --> 00:07:51.930
Pepijn van der Laan: The Cyber Resilience Act is, of course, part of a broader framework of EU regulations that are approaching fast.

44
00:07:51.990 --> 00:07:59.040
Pepijn van der Laan: where already you see here for Cyber Resilience Act the deadlines which are coming up.

45
00:07:59.040 --> 00:08:19.000
Pepijn van der Laan: And we see that this is typically one of the things that is that is on the radar of of our clients, but definitely not the only ones. So if you're interested in any of the other ones on a number of those, we do also have Webinars which we recorded which are available through the through the Namco website.

46
00:08:19.370 --> 00:08:22.870
Pepijn van der Laan: Or otherwise, please reach out to our experts on that.

47
00:08:23.160 --> 00:08:24.070
Pepijn van der Laan: So…

48
00:08:24.140 --> 00:08:35.129
Pepijn van der Laan: Cyber Resilience Act, yeah, what is it about? It's really about cybersecurity for products, to reduce the vulnerabilities in products with digital elements.

49
00:08:35.130 --> 00:08:54.960
Pepijn van der Laan: as they are called. So that means we're no longer talking only about hardware, but we're talking about a combination of hardware and software. Also,

remote data processing is a part of that when you talk about digital elements of products.

50
00:08:54.960 --> 00:09:08.279
Pepijn van der Laan: And the requirements, yeah, basically the Cyber Resilience Act is raising the bar there in terms of security and design by, by default, and that is both

51
00:09:08.300 --> 00:09:17.849
Pepijn van der Laan: In terms of the product as shipped, as well as the responsibility that, as a manufacturer, you have over the

52
00:09:17.850 --> 00:09:33.200
Pepijn van der Laan: both across the supply chain and over the life cycle of the product. I'll talk a little bit more about that in detail. Key date, first date is really September 11th, 2026, where

53
00:09:33.200 --> 00:09:51.030
Pepijn van der Laan: Later in this presentation, Gustavo will dive more into the specifics of the mandatory vulnerability disclosure and incident reporting, which comes with strict timelines. Also, always good to note in this kind of setting, there are really

54
00:09:51.030 --> 00:10:00.960
Pepijn van der Laan: potentially significant fines related to non-compliance, upping the importance also of this topic.

55
00:10:02.180 --> 00:10:03.200
Pepijn van der Laan: So…

56
00:10:04.270 --> 00:10:18.990

Pepijn van der Laan: to be a bit more explicit about, yeah, about the… the products with digital elements, and, how the Cyber Resilience Act thinks about that. So, on the left here, you see…

57
00:10:19.200 --> 00:10:27.690
Pepijn van der Laan: how the Cyber Resilience Act thinks about, the object of conformity. So, yes, that is the device itself.

58
00:10:27.690 --> 00:10:36.709
Pepijn van der Laan: It is also the software that is on the device or supporting software that might be in the app.

59
00:10:36.710 --> 00:10:53.190
Pepijn van der Laan: as well as remote data processing solutions. So this is not only about the data that is on the device, but also about data that is processed, but which is essential for how the device works.

60
00:10:54.580 --> 00:10:58.449
Pepijn van der Laan: So, that is really the object of conformity. If you look at

61
00:10:58.450 --> 00:11:09.159
Pepijn van der Laan: the responsibility, and it's really a life cycle responsibility. So that starts with the design in terms of secure design practices.

62
00:11:09.160 --> 00:11:18.639
Pepijn van der Laan: and development practices, but also the, the sourcing of, of components. So basically,

63
00:11:19.100 --> 00:11:35.289

Pepijn van der Laan: as a manufacturer, you need to be aware of the vulnerabilities that you're also inheriting through the, through the supply chain, which makes also concepts like the Software Bill of Materials, yeah, very relevant and very important in

64
00:11:35.290 --> 00:11:40.259
Pepijn van der Laan: ensuring conformity. And in the end, yeah, when you are

65
00:11:40.610 --> 00:11:52.209
Pepijn van der Laan: product is out in the market, in production, there is, basically, a continued responsibility also for the cybersecurity, so…

66
00:11:52.210 --> 00:11:56.779
Pepijn van der Laan: the cybersecurity, the Cyber Resilience Act there talks about

67
00:11:56.780 --> 00:12:15.360
Pepijn van der Laan: concept like a support period. So you need to be able to ensure that over that period you also ensure the security of the product. So in a number of ways here you see that also the regulation goes beyond just

68
00:12:15.630 --> 00:12:30.479
Pepijn van der Laan: a simple, check the product when it comes to market, but really stretches also into, more, process and organizational, requirements. We'll talk a little bit more about that, later as, as well.

69
00:12:32.220 --> 00:12:41.309
Pepijn van der Laan: Good to pinpoint also is that there are a couple of links to, to other regulations which are, which are important.

70
00:12:41.530 --> 00:12:52.429

Pepijn van der Laan: So one is the, radio equipment, directive, which is, of course, also about, devices communicating,

71
00:12:52.750 --> 00:13:09.910
Pepijn van der Laan: So there you see a partial overlap of responsibilities. In the end, it's envisioned that the CRA will take over the role from the RED directive and also is broader in terms of the requirements.

72
00:13:10.100 --> 00:13:11.000
Pepijn van der Laan: The.

73
00:13:11.380 --> 00:13:21.979
Pepijn van der Laan: So there… Compliance towards REST helps you towards compliance with CRA, but it's definitely, in many cases, not sufficient.

74
00:13:22.350 --> 00:13:38.840
Pepijn van der Laan: Then towards the AI Act, there's also a connection between the CRA and the AI Act, mostly from the security requirements that are in the AI Act.

75
00:13:38.860 --> 00:13:55.060
Pepijn van der Laan: at the moment, where basically conformity with CRA gives you the presumption of conformity on the cybersecurity requirements of the AI Act, so that basically helps an additional incentive to focus on that

76
00:13:55.200 --> 00:13:58.469
Pepijn van der Laan: on that CRA compliance as well.

77
00:13:58.870 --> 00:14:18.149
Pepijn van der Laan: There are a number of specific product categories, which have, which have exceptions. I'm not going to go into these for, for this pro- for this,

presentation, but it's good to be aware of that in some cases, there are those type of sectoral,

78
00:14:18.790 --> 00:14:21.700
Pepijn van der Laan: category specific regulations.

79
00:14:25.690 --> 00:14:45.180
Pepijn van der Laan: First thing that's important to realize is that the CRA basically discriminates between different type of products, critical products, important products, default products, where most products are expected to fall in the default category. And that is

80
00:14:45.730 --> 00:14:52.599
Pepijn van der Laan: Basically determined based on the core functionality of the product, the product with digital elements.

81
00:14:52.600 --> 00:15:11.139
Pepijn van der Laan: Where you really see that more important products and more critical products in terms of their cybersecurity function get into a higher class. Why is this important? This is important because it determines the path towards conformity that you have.

82
00:15:11.360 --> 00:15:13.840
Pepijn van der Laan: Basically, for,

83
00:15:14.750 --> 00:15:32.950
Pepijn van der Laan: For products that are default, that are not even class one, you can do self assessment. Same if you follow harmonized standards for class one, for class two, and for critical products, you get really into the…

84

00:15:32.950 --> 00:15:49.569
Pepijn van der Laan: certification schemes and notified bodies with mandatory third-party assessments. So this is quite an important first step to take. Also, this one we'll not dive into deeper at this moment.

85
00:15:49.580 --> 00:16:03.779
Pepijn van der Laan: What we'll dive into deeper is looking at the total set of requirements and what particular out of those requirements is it that is in that first batch of requirements that become relevant.

86
00:16:03.910 --> 00:16:05.060
Pepijn van der Laan: Gustavo.

87
00:16:06.800 --> 00:16:13.079
Gustavo Sanchez: Yes, now let's dive deeper on the actual obligations per September 11th.

88
00:16:13.360 --> 00:16:27.010
Gustavo Sanchez: So just as an overview, these are certain milestones that need to be achieved. But they are, of course, a subset of all the obligations that eventually will compound into full compliance.

89
00:16:27.100 --> 00:16:34.010
Gustavo Sanchez: And these milestones are publicly disclosing information about vulnerabilities, both

90
00:16:34.150 --> 00:16:38.450
Gustavo Sanchez: preview prior information before and after the mitigations.

91
00:16:38.750 --> 00:16:47.750

Gustavo Sanchez: And for this, strictly related to this, we have to ensure the coordinated vulnerability disclosure process.

92
00:16:48.290 --> 00:16:51.640
Gustavo Sanchez: Both in implementation and in policy-wise.

93
00:16:51.740 --> 00:17:03.289
Gustavo Sanchez: So we need to provide a channel for externals to be able to report vulnerabilities through a specific single point of contact.

94
00:17:03.370 --> 00:17:11.900
Gustavo Sanchez: And eventually we need to be able to disclose information through this same point.

95
00:17:12.010 --> 00:17:17.349
Gustavo Sanchez: This is something also related to general contact information of the manufacturer.

96
00:17:17.579 --> 00:17:21.040
Gustavo Sanchez: That goes along with the previous points.

97
00:17:21.200 --> 00:17:29.729
Gustavo Sanchez: Then, yeah, in the box here on the right hand side, you can see how indeed this is a smaller portion of the full compliance cycle.

98
00:17:30.340 --> 00:17:37.500
Gustavo Sanchez: In general, there is no need to ensure full vulnerability handling.

99
00:17:37.960 --> 00:17:47.989

Gustavo Sanchez: Other regulations may apply here, but eventually for CRA, right now we are looking at vulnerability disclosure.

100
00:17:48.150 --> 00:17:52.590
Gustavo Sanchez: And for example, not SBOMs, even though they are related.

101
00:17:53.040 --> 00:17:54.490
Gustavo Sanchez: Next slide, please.

102
00:17:55.520 --> 00:17:57.679
Pepijn van der Laan: Yes, perfect. So,

103
00:17:58.210 --> 00:18:12.620
Pepijn van der Laan: Let me see. So, that's the first view on what is coming at you towards that September 11th deadline. In the meantime, before we dive deeper into that, also curious where

104
00:18:12.620 --> 00:18:26.819
Pepijn van der Laan: where you all are with respect to, your preparations for the, for the CRA compliance. So, five, options here to, to choose from. Yeah, are you either just, just starting to learn.

105
00:18:26.820 --> 00:18:38.189
Pepijn van der Laan: Exploring what it takes, almost ready for the September 11 deadline. Are you already ahead of the game, working on the December obligations?

106
00:18:38.190 --> 00:18:50.399
Pepijn van der Laan: Or are you maybe even already fully set for compliance? Curious to hear from you. And at the end of the webinar, we'll also

107
00:18:51.700 --> 00:18:58.450
Pepijn van der Laan: Basically, tell you what, what your… Go webinar listeners!

108
00:18:58.680 --> 00:19:03.960
Pepijn van der Laan: have filled in on this so that you also have a bit of a view of.

109
00:19:04.320 --> 00:19:06.699
Pepijn van der Laan: Yeah, of how this, how this continues.

110
00:19:06.940 --> 00:19:21.650
Pepijn van der Laan: So, with that… Yeah, let's really kind of dive even further into those September 11 requirements. Gustavo.

111
00:19:22.720 --> 00:19:23.940
Gustavo Sanchez: Yes, great.

112
00:19:24.070 --> 00:19:41.000
Gustavo Sanchez: So let's talk about what will be reported in detail. So we have two different items. We have vulnerabilities and incidents, and we have specific technicalities that actually enforce whether these have to be reported or not.

113
00:19:41.140 --> 00:19:45.709
Gustavo Sanchez: So, for vulnerabilities, we have the concept of actively exploited.

114
00:19:46.030 --> 00:19:54.320
Gustavo Sanchez: So, those relate to those vulnerabilities that are known to be currently exploited by malicious actors.

115

00:19:54.860 --> 00:20:09.980
Gustavo Sanchez: In related to incidents, the severity essentially highlights that some of the assets of the product with digital elements have been compromised. There was a severe impact on them.

116
00:20:10.490 --> 00:20:24.270
Gustavo Sanchez: So what this means is that if we receive through a coordinated vulnerability disclosure, we receive a vulnerability that was not actively exploited, then we are not required to report it.

117
00:20:24.520 --> 00:20:39.350
Gustavo Sanchez: One example will be a zero day. So if a researcher get us aware of a zero day vulnerability, but was never exploited in the wild, then this is not to be reported.

118
00:20:39.550 --> 00:20:40.870
Gustavo Sanchez: For incidents.

119
00:20:41.340 --> 00:20:53.219
Gustavo Sanchez: We have certain details, for example, if a specific cyber incident negatively affected a capability that we are trying to protect.

120
00:20:53.300 --> 00:21:03.629
Gustavo Sanchez: then is is problematic and might be severe. But also in in this line, if the incident facilitates

121
00:21:03.730 --> 00:21:07.080
Gustavo Sanchez: Code execution, remote execution of code.

122
00:21:07.400 --> 00:21:14.170

Gustavo Sanchez: obviously from a malicious perspective, then this will also be labeled as severe.

123
00:21:14.760 --> 00:21:16.989
Gustavo Sanchez: Alright, in terms of incident.

124
00:21:17.470 --> 00:21:18.580
Gustavo Sanchez: Next slide.

125
00:21:21.150 --> 00:21:28.080
Gustavo Sanchez: Now… Once we have an incident reaching our inbox, What is the timeline?

126
00:21:28.260 --> 00:21:29.090
Gustavo Sanchez: So…

127
00:21:29.250 --> 00:21:39.799
Gustavo Sanchez: the, the, the, the timestamp or the, the, the time starts running not at, exploit, exploiting time. So if, a vulnerability

128
00:21:39.840 --> 00:21:59.349
Gustavo Sanchez: was actually exploited in the past, but we are just aware of this, then that's when the time starts counting. So the next deadline that will come will be in 24 hours from that point where we need to disclose an early warning.

129
00:22:00.260 --> 00:22:01.170
Gustavo Sanchez: Then…

130
00:22:01.340 --> 00:22:13.799

Gustavo Sanchez: There will be a more detailed notification including information about the incident or vulnerability and an initial assessment in 72 hours.

131
00:22:14.280 --> 00:22:27.780
Gustavo Sanchez: And at this point, then we have two branches. So if we are talking about the vulnerability, then we need to be able to work towards corrective measures, so control mitigations.

132
00:22:28.220 --> 00:22:33.310
Gustavo Sanchez: And, and provide a final report within 14 days.

133
00:22:33.570 --> 00:22:38.350
Gustavo Sanchez: In terms of a… Incident, we will have one month.

134
00:22:38.490 --> 00:22:45.580
Gustavo Sanchez: to convey all the information, so due diligence, Forensics, and so on, into a final report.

135
00:22:45.710 --> 00:22:46.880
Gustavo Sanchez: Within one month.

136
00:22:48.070 --> 00:22:49.020
Gustavo Sanchez: Next slide.

137
00:22:52.440 --> 00:22:55.640
Gustavo Sanchez: For this, we need to discuss the topic of

138
00:22:55.830 --> 00:23:06.180

Gustavo Sanchez: vulnerability and incident documentation. So, record keeping. So, what are we actually storing, and what principles are behind this? So, we have these three

139
00:23:06.230 --> 00:23:16.029
Gustavo Sanchez: Cornerstones, we have traceability, testability, and the capability for the incident or the vulnerability to be treated.

140
00:23:16.600 --> 00:23:26.199
Gustavo Sanchez: With these three concepts, we were able to, in order to reach these three milestones, we need to collect some information.

141
00:23:26.820 --> 00:23:39.209
Gustavo Sanchez: This is a long list, but here are focusing on those fields, specifically prioritized for September 11th deadline.

142
00:23:39.500 --> 00:23:46.009
Gustavo Sanchez: For example, identifiers for the vulnerability or the incident, the type.

143
00:23:46.290 --> 00:23:48.310
Gustavo Sanchez: The status, and so on.

144
00:23:48.740 --> 00:24:02.710
Gustavo Sanchez: As you can see here, some of these pieces of data are just metadata. Quickly available from the report, even sometimes generated such a timestamp.

145
00:24:02.860 --> 00:24:04.950
Gustavo Sanchez: But some others need to be…

146
00:24:05.140 --> 00:24:17.290
Gustavo Sanchez: address in a more comprehensive way. For instance, the risk level has to be computed by merging the likelihood and the impact of a vulnerability.

147
00:24:17.420 --> 00:24:28.630
Gustavo Sanchez: And some others will require a bit more of diligence from the manufacturer's side, for example, the root cause, which might not be straightforward.

148
00:24:28.750 --> 00:24:46.259
Gustavo Sanchez: But important to highlight for December 2027, meaning full compliance, we will have to address other pieces of information such as identifiers linking SBOMs to the components affected and so on.

149
00:24:47.010 --> 00:24:48.110
Gustavo Sanchez: Next slide.

150
00:24:51.100 --> 00:24:54.419
Gustavo Sanchez: So, what is the connection between

151
00:24:54.820 --> 00:25:00.989
Gustavo Sanchez: these different concepts that, compound into vulnerability handling. So, we have…

152
00:25:01.160 --> 00:25:05.409
Gustavo Sanchez: as mentioned, the coordinated vulnerability disclosure.

153
00:25:05.600 --> 00:25:09.860
Gustavo Sanchez: This is a framework and a structure for externals.

154
00:25:09.980 --> 00:25:25.130
Gustavo Sanchez: to be able to report vulnerabilities, because not all vulnerabilities will be identified from the inside, from the developers themselves, from the institution that is the manufacturer, right? So, in many cases.

155
00:25:25.250 --> 00:25:35.900
Gustavo Sanchez: researchers, ethical hackers, or incident response teams will chip in, will contribute to To make the products safer.

156
00:25:36.260 --> 00:25:41.100
Gustavo Sanchez: For example, in Europe, there are more than 500

157
00:25:41.210 --> 00:25:52.300
Gustavo Sanchez: incident response teams, and many of them cluster within networks, and it is common that threat intelligence or vulnerability intelligence is shared among them.

158
00:25:53.030 --> 00:25:53.970
Gustavo Sanchez: Once.

159
00:25:54.780 --> 00:26:04.560
Gustavo Sanchez: any of these sources provide a specific initial report, then the This information will get assessed.

160
00:26:04.760 --> 00:26:07.580
Gustavo Sanchez: We'll get triaged, or prioritized.

161
00:26:07.730 --> 00:26:15.270

Gustavo Sanchez: And there will be remediation with the release, the corresponding release, and there will be lessons learned.

162
00:26:15.840 --> 00:26:16.780
Gustavo Sanchez: Then…

163
00:26:17.080 --> 00:26:31.400
Gustavo Sanchez: In order to make this happen, we need documentation, which is the evidence that the manufacturers need to record, need to store in order to eventually prove that vulnerabilities incidents were treated systematically.

164
00:26:31.710 --> 00:26:33.130
Gustavo Sanchez: As per the CRA.

165
00:26:33.260 --> 00:26:52.660
Gustavo Sanchez: And the final goal of this is to be able to report the vulnerabilities when actively exploited or the incidents when they are severe. This will be reported directly through ENISA.

166
00:26:53.080 --> 00:26:59.429
Gustavo Sanchez: as we will see next. But this relates to the CRA article 14.

167
00:27:00.460 --> 00:27:01.850
Gustavo Sanchez: Next slide, please.

168
00:27:02.400 --> 00:27:03.180
Gustavo Sanchez: Right.

169
00:27:03.300 --> 00:27:08.370

Gustavo Sanchez: So… Same thing for the vulnerability disclosure policy.

170
00:27:08.610 --> 00:27:14.030
Gustavo Sanchez: and inherent process, we have three cornerstones. Accessibility.

171
00:27:14.390 --> 00:27:15.910
Gustavo Sanchez: Confidentiality.

172
00:27:16.120 --> 00:27:23.490
Gustavo Sanchez: And the capability to acknowledge receivable and further items within the process.

173
00:27:23.760 --> 00:27:25.479
Gustavo Sanchez: in… in practice.

174
00:27:25.850 --> 00:27:28.399
Gustavo Sanchez: We have to ensure,

175
00:27:28.600 --> 00:27:38.149
Gustavo Sanchez: this through certain requirements. For example, a vulnerability reporter has to be able to submit anonymously.

176
00:27:38.370 --> 00:27:43.709
Gustavo Sanchez: So this means we cannot request mandatory personal fields in the form.

177
00:27:43.890 --> 00:27:49.820
Gustavo Sanchez: And their identities will not be linked to the submission.

178
00:27:50.410 --> 00:28:00.630
Gustavo Sanchez: Then some other interesting requirements here. For instance, we have to be able to trace the

179
00:28:01.140 --> 00:28:03.160
Gustavo Sanchez: the, the, the report.

180
00:28:03.430 --> 00:28:07.579
Gustavo Sanchez: And the the form has to be easy to access.

181
00:28:07.690 --> 00:28:09.889
Gustavo Sanchez: No login, no blockers.

182
00:28:10.170 --> 00:28:22.789
Gustavo Sanchez: And eventually, if we are doing this right, we will be able to acknowledge the receipt of the information to the user who reported it.

183
00:28:22.900 --> 00:28:40.590
Gustavo Sanchez: This is quite common in responsible vulnerability disclosure to link the reporter to an eventual fix and even publicly disclose that a specific researcher or institution identified this.

184
00:28:40.660 --> 00:28:43.350
Gustavo Sanchez: Prior and notified through the.

185
00:28:43.790 --> 00:28:45.500
Gustavo Sanchez: proper ways.

186

00:28:45.660 --> 00:28:50.660
Gustavo Sanchez: And yeah, this contributes towards a healthy security community.

187
00:28:51.400 --> 00:28:52.370
Gustavo Sanchez: Next slide.

188
00:28:53.190 --> 00:29:02.680
Gustavo Sanchez: We have discussed briefly that the point of reporting is ENISA, but more in detail, it is called Single Reporting Platform.

189
00:29:03.770 --> 00:29:18.690
Gustavo Sanchez: This is a web application web form accessible through official ENISA websites and the information will be directed to the incident response team of the

190
00:29:18.970 --> 00:29:20.300
Gustavo Sanchez: Relevant country.

191
00:29:20.860 --> 00:29:31.290
Gustavo Sanchez: And at the same time, this information will be readily ready to be accessed by ENISA, which helps towards coordination.

192
00:29:31.570 --> 00:29:34.850
Gustavo Sanchez: A bit more information on this, so…

193
00:29:35.140 --> 00:29:49.600
Gustavo Sanchez: there was a call for tender to to find a to award a contract for the development and design and implementation of the of the single reporting platform, and it was assigned to a

194

00:29:49.700 --> 00:29:54.929
Gustavo Sanchez: to a trilateral consortium. 3 entities are working on this at the moment.

195
00:29:55.100 --> 00:30:03.640
Gustavo Sanchez: And it is scheduled to be operational by the very final date, so 11th September.

196
00:30:03.850 --> 00:30:07.859
Gustavo Sanchez: 2026, but there will be a potential testing period.

197
00:30:08.530 --> 00:30:17.560
Gustavo Sanchez: Now, more information on this related to manuals and guidelines will be provided in principle.

198
00:30:17.940 --> 00:30:26.720
Gustavo Sanchez: But, seems to be a delay on this, so we will keep an eye there and, and, and address this.

199
00:30:26.980 --> 00:30:29.660
Gustavo Sanchez: Accordingly, once information arrives.

200
00:30:30.160 --> 00:30:31.330
Gustavo Sanchez: Next slide.

201
00:30:32.190 --> 00:30:49.409
Gustavo Sanchez: Right. So for you, what are the minimal capabilities that you need to put in place in order to fulfill these reporting obligations according to the deadline? Well, so first we have related to detection and classification.

202
00:30:49.510 --> 00:30:56.159
Gustavo Sanchez: Of vulnerabilities and incidents, we need to put this in place, so we need to be able to detect and classify.

203
00:30:56.470 --> 00:31:01.550
Gustavo Sanchez: what is coming through the vulnerability reporting flows.

204
00:31:02.110 --> 00:31:04.369
Gustavo Sanchez: And then, we need to…

205
00:31:04.620 --> 00:31:09.479
Gustavo Sanchez: have a specific workflow or steps.

206
00:31:09.650 --> 00:31:12.830
Gustavo Sanchez: That they start with detection, classification.

207
00:31:13.140 --> 00:31:17.660
Gustavo Sanchez: Addressing the specific deadlines, and producing an eventual final report.

208
00:31:17.820 --> 00:31:23.760
Gustavo Sanchez: There is also an additional, necessity here, which is informing users.

209
00:31:24.240 --> 00:31:27.270
Gustavo Sanchez: Which includes providing mitigations.

210
00:31:27.700 --> 00:31:32.000
Gustavo Sanchez: So this has to also be ambitions from the beginning.

211
00:31:32.400 --> 00:31:43.129
Gustavo Sanchez: And then we have responsible roles, of course, so we need to assign roles to specific stakeholders within the institutions so that there is a proper decision making process.

212
00:31:43.260 --> 00:31:45.939
Gustavo Sanchez: And we know exactly who is submitting.

213
00:31:46.540 --> 00:31:48.339
Gustavo Sanchez: And, then…

214
00:31:48.860 --> 00:32:01.369
Gustavo Sanchez: We need a bit more on the operational side of things. We need access to this SRP platform, and we need to have the ability to create reports.

215
00:32:01.950 --> 00:32:09.110
Gustavo Sanchez: And yeah, beyond the requirements that I have mentioned just now.

216
00:32:09.110 --> 00:32:10.840
Pepijn van der Laan: Sorry.

217
00:32:10.840 --> 00:32:15.130
Gustavo Sanchez: Yeah, no worries. Just finishing. So we need to collect timestamps.

218
00:32:15.290 --> 00:32:18.200
Gustavo Sanchez: And submit, and be ready for follow-ups.

219

00:32:18.470 --> 00:32:22.890
Gustavo Sanchez: Then, yeah, specifically about sharing.

220
00:32:23.020 --> 00:32:32.460
Gustavo Sanchez: we need to provide mitigation instructions to users. This is the end goal, and this is when the cycle will be closed.

221
00:32:34.280 --> 00:32:36.640
Gustavo Sanchez: With this, we can continue. Awesome. Yep.

222
00:32:36.950 --> 00:33:01.490
Pepijn van der Laan: Yeah, perfect. So thanks a lot, Gustavo, for that deep dive into the requirements for September. I already saw in the corner of my eye quite some questions also in the webinar chat. So yeah, keep those coming. We'll get to those, maybe not all of them, depending on how many there are.

223
00:33:01.490 --> 00:33:03.869
Pepijn van der Laan: But we'll do our best.

224
00:33:03.870 --> 00:33:07.339
Pepijn van der Laan: But before we dive into the Q&A,

225
00:33:07.340 --> 00:33:16.269
Pepijn van der Laan: Let's also briefly talk about how to get started there, because Gustavo already mentioned some of the

226
00:33:16.500 --> 00:33:33.309
Pepijn van der Laan: has some of the capabilities that are also needed in order to comply with the CRA. And I think that touches upon, yeah, really one of the important points that we see, and we see it in more EU regulation.

227
00:33:33.310 --> 00:33:45.359
Pepijn van der Laan: yeah, for example, in the AI Act, but with CRA is really one of the first ones where this takes prominence. That combination of kind of looking and acknowledging that products in

228
00:33:45.360 --> 00:33:47.820
Pepijn van der Laan: In today's world are not just products.

229
00:33:47.820 --> 00:34:12.809
Pepijn van der Laan: but also come together with a life cycle and also often a support period. So that means that next to the more traditional product requirements, the CRA also has quite stringent process requirements in terms of vulnerability assessments, testing and review, information sharing.

230
00:34:12.810 --> 00:34:13.370
Pepijn van der Laan: That's…

231
00:34:13.370 --> 00:34:24.470
Pepijn van der Laan: yeah, security practices that you need to implement at an organizational level. So, what is asked from, yeah, you as an organization, if you're,

232
00:34:24.889 --> 00:34:44.070
Pepijn van der Laan: If you're a manufacturer, it's really about integrating the product security and the organizational governance. It's about really moving from ad hoc controls at the moment that you bring a product to market to really a repeatable and documented process where you have control over the full process.

233
00:34:44.070 --> 00:34:49.840

Pepijn van der Laan: full life cycle, so that links, engineering, compliance, and operational security.

234
00:34:49.840 --> 00:34:50.739
Pepijn van der Laan: And.

235
00:34:50.739 --> 00:34:59.639
Pepijn van der Laan: So really that ongoing continuous vulnerability management and that connecting the product life cycle.

236
00:34:59.640 --> 00:35:18.350
Pepijn van der Laan: That are the important things that also we see some of our clients have to take really steps in order to close the gap there and make sure that they're ready for the Cyber Resilience Act.

237
00:35:18.530 --> 00:35:19.290
Pepijn van der Laan: And.

238
00:35:19.810 --> 00:35:20.820
Pepijn van der Laan: So…

239
00:35:22.220 --> 00:35:35.509
Pepijn van der Laan: what are some of the common challenges there? Yeah, it's about, unclarity about standards. We didn't talk about standards that much, this, in this webinar, but,

240
00:35:36.030 --> 00:35:44.100
Pepijn van der Laan: Yeah, I think, good to mention that, that standards for, for CRA are not yet, yet harmonized.

241
00:35:44.100 --> 00:35:59.609
Pepijn van der Laan: So that provides a bit of a challenge. Doesn't mean that you cannot do anything, but you need to think about how and when to do it. Decentralized processes, which is something that if you want to basically show the control, in particular on those process.

242
00:35:59.610 --> 00:36:00.870
Pepijn van der Laan: Dimensions.

243
00:36:01.070 --> 00:36:14.639
Pepijn van der Laan: Yeah, that can be a challenge to, to get your, your evidence in, in place. Limited visibility in, on software components, also something that, if you want to basically assure

244
00:36:14.640 --> 00:36:29.309
Pepijn van der Laan: the compliance of a product with digital elements. Super important, but sometimes, yeah, not something that has been built from the ground up as part of the standard way of working to the level that it's currently required.

245
00:36:29.310 --> 00:36:34.140
Pepijn van der Laan: Resources and capability constraints, yeah, of course.

246
00:36:34.140 --> 00:36:51.090
Pepijn van der Laan: Yeah, there's a lot going on in the world of regulation and compliance, so resources are scarce, technical teams are always, are always busy, so, definitely a challenge how you plan a resource for, for that, but also the organizational readiness in terms of the.

247
00:36:51.090 --> 00:37:02.929

Pepijn van der Laan: Proactive thinking about, about security and making sure that the, that the right cross-functional accountability and collaboration are in place in your, in your organization.

248
00:37:02.930 --> 00:37:03.720
Pepijn van der Laan: And.

249
00:37:04.300 --> 00:37:05.370
Pepijn van der Laan: So…

250
00:37:06.270 --> 00:37:18.030
Pepijn van der Laan: To support clients on that journey, we have developed a six-step approach, where the first step, in terms of discovery and alignment, is typically for a bit

251
00:37:18.030 --> 00:37:33.790
Pepijn van der Laan: larger corporations who have a complex product portfolio. Otherwise, you can step directly into assessing the applicability and the requirements. From there, understanding where are you versus those requirements, gap analysis.

252
00:37:33.790 --> 00:37:44.289
Pepijn van der Laan: Working on the remediation and control, towards, in the end, validation, testing, and certification, where it's important to realize that, indeed, for the default category.

253
00:37:44.290 --> 00:37:54.029
Pepijn van der Laan: the self-declaration is sufficient. If that's not sufficient, if you're in an important or critical category, then

254
00:37:54.350 --> 00:38:12.319

Pepijn van der Laan: we always, also, in collaboration with our, our colleagues in the EMCO group, assure that we, maintain proper, proper impartiality, of course. And in the end, yeah, enhancement and monitoring, yeah, this is really something over the life cycle, so…

255
00:38:12.320 --> 00:38:16.660
Pepijn van der Laan: That also holds for everything that you do towards compliance.

256
00:38:16.660 --> 00:38:28.640
Pepijn van der Laan: So specifically for the CRA, what we see at the moment is because of those two deadlines that are approaching, we often see a two.

257
00:38:28.640 --> 00:38:41.900
Pepijn van der Laan: two-tiered approach, where on the one hand, companies are looking at kind of, yeah, the fast lane for controls towards getting ready for September 2026, but at the same time, yeah, you see

258
00:38:41.900 --> 00:38:59.330
Pepijn van der Laan: there's more time towards December 2027, but also, if you remember Gustavo's slide from earlier, a much longer list of requirements. So you cannot typically sit still. So where to start on that second part?

259
00:39:00.230 --> 00:39:08.480
Pepijn van der Laan: basically going back to the essence of the Cyber Cyber Resilience Act. A lot of the

260
00:39:08.660 --> 00:39:19.140
Pepijn van der Laan: requirements are phrased in a way that they are based on the level of risk. So

261

00:39:19.710 --> 00:39:35.970
Pepijn van der Laan: Compliance with the Cyber Resilience Act starts with understanding your cyber risk. So a cyber risk assessment is typically a foundational element for the full compliance of CRA, so that is the recommendation often to start at

262
00:39:35.970 --> 00:39:51.570
Pepijn van der Laan: Alongside working on the reporting controls, really looking at the cyber, yeah, at your cyber risk assessment, and, and making sure that based on that you can drive, okay, what are the specific controls that I need to have on,

263
00:39:51.960 --> 00:39:53.329
Pepijn van der Laan: On the product level.

264
00:39:53.790 --> 00:39:54.620
Pepijn van der Laan: So.

265
00:39:55.140 --> 00:40:05.279
Pepijn van der Laan: That is what we wanted to share about the CRA, the deadline that's upcoming, and a little bit of a sneak peek at what's coming after that.

266
00:40:06.560 --> 00:40:07.570
Pepijn van der Laan: So…

267
00:40:07.820 --> 00:40:24.779
Pepijn van der Laan: we will do a bit of Q&A, now, but, also want to invite you, if you really want to take that, that next step, don't wait for, for September, but, really reach out to our, to our experts and,

268
00:40:24.780 --> 00:40:28.169
Pepijn van der Laan: We'll talk with you about, about how to get there.

269
00:40:28.500 --> 00:40:29.520
Pepijn van der Laan: So.

270
00:40:29.820 --> 00:40:36.679
Pepijn van der Laan: And of course, from an EMCO Digital perspective, you can always follow us and

271
00:40:36.760 --> 00:40:56.569
Pepijn van der Laan: get running updates on everything that's happening towards towards digital compliance but with that let me stop sharing the the screen and go towards the towards the questions that we have received in the

272
00:40:56.740 --> 00:41:05.979
Pepijn van der Laan: In the chat, I see quite a list, so that is good, that's good news. Maybe taking, taking the first question there,

273
00:41:07.240 --> 00:41:22.329
Pepijn van der Laan: So, about software versus hardware, and what does that mean in terms of a product with digital elements? Can that be software only, or is hardware necessary? Gustavo, maybe you can explain a bit about that.

274
00:41:22.990 --> 00:41:36.060
Gustavo Sanchez: Yes, so the existence of hardware is not the only requirement, meaning, yes, indeed, software that qualifies as a product with digital elements, maybe within a scope.

275
00:41:36.240 --> 00:41:43.760
Gustavo Sanchez: The recommendation here is to assess the software products that you're making available in the market.

276
00:41:43.880 --> 00:41:55.900
Gustavo Sanchez: Based on… so, based on the Annex 3, 4, and if they are not there, then might be qualified as default, but still indeed within scope.

277
00:41:58.330 --> 00:42:16.730
Pepijn van der Laan: Perfect. And maybe in connection to that, I also see a follow-up question here about the remote data processing solutions. Have we mentioned those before? If you could also explain maybe a bit about what is exactly meant with that.

278
00:42:16.960 --> 00:42:22.680
Gustavo Sanchez: Yes, there are a series of… Concept that will be…

279
00:42:22.870 --> 00:42:28.190
Gustavo Sanchez: related to remote data processing. So the things like cloud services.

280
00:42:28.580 --> 00:42:40.259
Gustavo Sanchez: APIs, telemetry… Portals, so at the end, these are also enhancing the attack surface, and therefore,

281
00:42:40.450 --> 00:42:48.540
Gustavo Sanchez: within the context of the CRA. And indeed, the product, if the product depends on them, will be part of risk assessment.

282
00:42:49.860 --> 00:43:05.489
Pepijn van der Laan: Yeah, thanks Gustavo. So really kind of had a dependence on that and kind of had the digital elements being essential for the functioning of the products. That's really an important criterion there.

283

00:43:05.490 --> 00:43:26.080
Pepijn van der Laan: from there going into mention of the machinery regulation, which will come mandatory. So maybe I can give a first answer on that and then Gustavo feel free to add on. So machinery regulation is indeed, of course.

284
00:43:26.270 --> 00:43:40.840
Pepijn van der Laan: A different one from a different angle. It also like more, more general safety, regulations that you see within Europe is increasingly, aware of.

285
00:43:41.390 --> 00:43:51.860
Pepijn van der Laan: the digitization of the world, and in this case, machinery. So, typically, you see those regulations serving as a backstop

286
00:43:51.860 --> 00:44:07.649
Pepijn van der Laan: in terms of defining what does safety mean. And digital safety becomes part of the definition of safety as it is in the machinery regulation. Similarly.

287
00:44:07.650 --> 00:44:23.199
Pepijn van der Laan: yeah, we're now talking about cyber security, but also about AI. We see a different, a similar tendency, both in the machinery regulation, but also, for example, in the general product safety regulation, that

288
00:44:24.130 --> 00:44:41.719
Pepijn van der Laan: even psychological safety due to AI is, is part of the definition of safety in those, in those regulations. So that means that, there's indeed, as, as asked here, quite an important relationship, but in

289
00:44:41.720 --> 00:44:49.920
Pepijn van der Laan: In general, it's fair to say that the machinery regulation is much more focused on the machine safety and

290
00:44:50.100 --> 00:44:56.210
Pepijn van der Laan: the cyber security aspects are really much more covered in the Cyber Resilience Act.

291
00:44:57.100 --> 00:44:57.740
Pepijn van der Laan: Yes.

292
00:44:57.740 --> 00:45:15.369
Gustavo Sanchez: Maybe to briefly add to this, so maybe the actual relation between the two of them can be understood by looking at the use case so For example, a cybersecurity compromise of a cyber physical system

293
00:45:15.390 --> 00:45:19.440
Gustavo Sanchez: Might create safety compromises in the operator.

294
00:45:19.770 --> 00:45:23.860
Gustavo Sanchez: So, both of them eventually overlap in that one.

295
00:45:24.190 --> 00:45:25.510
Gustavo Sanchez: Just to consider.

296
00:45:26.130 --> 00:45:31.119
Pepijn van der Laan: Yeah, thanks, Gustavo. Great, great addition.

297
00:45:31.130 --> 00:45:49.360
Pepijn van der Laan: And then from there, another question about the timeline as well, and that is about the obligations for September and December 2027, Gustavo, if those are also for products that are already deployed in the field.

298
00:45:49.450 --> 00:45:52.540
Pepijn van der Laan: Or only for, for new ones.

299
00:45:52.600 --> 00:45:58.520
Gustavo Sanchez: So, generally, yes, products, still within the support period.

300
00:45:59.230 --> 00:46:11.330
Gustavo Sanchez: will… but there are important nuances. So the… the… yeah, the reporting requirements for Article 14 indeed start applying from September 26.

301
00:46:11.640 --> 00:46:17.010
Gustavo Sanchez: But the full compliance within 27, and those products that are

302
00:46:17.620 --> 00:46:22.509
Gustavo Sanchez: that were placed before are not automatically recertified.

303
00:46:22.820 --> 00:46:29.609
Gustavo Sanchez: But yeah, the manufacturers may still have the… The obligation, the need…

304
00:46:30.640 --> 00:46:36.189
Gustavo Sanchez: Yeah, for vulnerabilities discovered and supported products retroactively.

305
00:46:36.660 --> 00:46:49.750
Gustavo Sanchez: Yeah, furthermore, a product that is substantially refactored will also trigger new obligations, even if you certify your product

306

00:46:50.000 --> 00:46:56.280
Gustavo Sanchez: So they… And maybe in 3 months you will have to trigger a new risk assessment.

307
00:46:56.430 --> 00:47:03.859
Gustavo Sanchez: So the timeline, as you can see, is not only for future products exclusively.

308
00:47:05.960 --> 00:47:24.979
Pepijn van der Laan: Perfect. So, I see that there is quite a list of questions still, but I propose that we just do, just do one more, and then, round off for the day, and, questions that we didn't get to, yeah, we'll reach out, afterwards,

309
00:47:24.980 --> 00:47:27.439
Pepijn van der Laan: For, for a follower.

310
00:47:27.440 --> 00:47:36.490
Pepijn van der Laan: So, yeah, and that's, I think, a nice question, because it also ties into some of the things that you were talking about, Gustavo, with the…

311
00:47:36.490 --> 00:47:48.850
Pepijn van der Laan: with the timeline. Aware of incident, yeah, does that mean that you receive an email, or does it mean that you have validated the information and, basically written a report,

312
00:47:49.330 --> 00:47:56.330
Pepijn van der Laan: When are you aware of the of the incident? And when starts, is it the time that starts ticking?

313
00:47:57.170 --> 00:48:08.320

Nemko Digital

Gustavo Sanchez: Yeah, very good question. So indeed, receiving an email or a form from a White Hat researcher will not start triggering the countdown.

314
00:48:08.550 --> 00:48:24.159
Gustavo Sanchez: It is indeed when there has been some sort of triage, some sort of initial validation. The reason behind this is because a specific report might be very preliminary or might be incomplete.

315
00:48:24.300 --> 00:48:28.559
Gustavo Sanchez: And and therefore there is this need to to replicate.

316
00:48:28.760 --> 00:48:38.390
Gustavo Sanchez: Yeah, and then… discover whether this was actually exploited, and so on. So yeah, the quick answer.

317
00:48:38.550 --> 00:48:48.409
Gustavo Sanchez: clicking on submit and receiving something in the inbox doesn't trigger the ticking of the clock. It is further steps.

318
00:48:50.270 --> 00:49:00.709
Pepijn van der Laan: Okay. Thank you, Gustavo. And thanks to all participants. Apologies for not getting to all the questions.

319
00:49:00.710 --> 00:49:13.860
Pepijn van der Laan: But, yeah, well, wish you a lot of luck in, and success in getting towards compliance for the, for the CRA, and if you need support on the way, feel free to reach out and,

320
00:49:13.980 --> 00:49:15.990
Pepijn van der Laan: Enjoy the rest of your day!

321
00:49:17.350 --> 00:49:18.980
Gustavo Sanchez: Thank you. Bye-bye.

322
00:49:19.630 --> 00:49:20.440
Pepijn van der Laan: Bye-bye.