MARSH

WEBVTT – Cyber

4
00:00:11.380 --> 00:00:22.419
Raul Munoz: Welcome back to Mining in 10 Minutes. I'm Raul Munoz at Marsh, and in today's episode, we're driving into one of the fastest growing risk categories in our industry, your cyber risk.

5
00:00:22.570 --> 00:00:39.739
Raul Munoz: As we all know, mining has gone an unremarkable digital transformation in the recent years. From autonomous trucks to remote monitoring to IoT sensors, real-time analytics, all of that technology has made operations safer and way more efficient.

6
00:00:39.920 --> 00:00:56.360
Raul Munoz: But it also opened the doors to what didn't exist before, the cyber risk. My guest today is Julian Ducloy, who is a cyber risk specialist at Marsh Risk, and works specifically with industrial and mining clients. So let's get into it. Thank you very much for joining me, Julian.

7
00:00:57.380 --> 00:00:58.919
Julien Ducloy: Thank you, Raul. Nice to be here.

8
00:01:00.000 --> 00:01:05.750
Raul Munoz: Let's start with the basics. What kinds of cyber risk should mining leaders be thinking about?

9
00:01:06.880 --> 00:01:09.920
Julien Ducloy: So, at a high level, there are two categories.

10
00:01:10.030 --> 00:01:28.580
Julien Ducloy: Targeted attacks, where a cybercriminal deliberately goes after a specific organization, generally because they know about a particular asset, they want access to valuable data, or they're seeking to cause disruption for competitive or geopolitical reasons.

11
00:01:28.920 --> 00:01:42.830
Julien Ducloy: And the other category is the untargeted or wide area attacks, where the attacker is essentially, like, casting a wide net. Ransomware deployed broadly, phishing campaigns, to get, access credentials.

12
00:01:42.830 --> 00:01:49.589
Julien Ducloy: Or vulnerability scanned through the web, and they're hoping to catch anyone who isn't adequately protected.

13
00:01:50.580 --> 00:02:07.299
Raul Munoz: It's interesting, because generally speaking, when… when we think about cyber attacks, we… mining doesn't necessarily… is not the first thing that comes… comes to mind. So what kind of, consequences could a successful cyber attack have for… specifically for mining companies?

14
00:02:07.900 --> 00:02:27.619
Julien Ducloy: They can be severe, and there's a wide range of consequences. We have seen a lot of incidents in the past, different type of incidents in mining industry, and at the most serious end, you're talking about attacks on the operational technology, so the systems that control the physical equipment.

15
00:02:27.650 --> 00:02:36.550
Julien Ducloy: And if an attacker gains access to a mining control system, they could manipulate the equipment behavior, create safety hazard, and disrupt production.

16
00:02:36.770 --> 00:02:51.320
Julien Ducloy: At the same time, the attack on the IT systems can result in theft of exploration data, financial information, production metrics as well, and this information has an enormous competitive value.

17
00:02:51.330 --> 00:03:07.199
Julien Ducloy: And last, I mean, we all heard about that, the ransomware attacks, that are targeting, both IT and OT system, actually maximize leverage and can be, pretty devastating.

18
00:03:07.900 --> 00:03:21.569
Raul Munoz: Yeah, you know, it's interesting, because when we think about, you know, the journey and the life cycle of a mining company, there's obviously different levels from exploration all the way through reclamations, and I think one of the most

19
00:03:21.570 --> 00:03:30.589
Raul Munoz: interesting chapters in the Resilience Guide is, the frameworks that are described in Chapter 3.

20
00:03:30.590 --> 00:03:48.299
Raul Munoz: Where, you know, we talk about, you know, those different exposures throughout the different, the different cycles. Can you perhaps walk us through, what some of those key stages are, and, and perhaps what are the things that clients should be thinking about, wherever stage they sit under?

21
00:03:48.980 --> 00:03:59.529
Julien Ducloy: Yeah, absolutely. The life cycle gives us a structure to understand the cyber exposure in the mining industry. So we're starting with exploration.

22
00:03:59.530 --> 00:04:06.239
Julien Ducloy: So this is a stage that people don't always think as cyber-exposed, but exploration data is incredibly valuable.

23
00:04:06.240 --> 00:04:21.120
Julien Ducloy: When we think about everything that is invested into exploration, and unauthorized access to site acquisition data or GIS system could cost a company a competitive advantage worth billions. And they might never know about it, in fact.

24
00:04:21.120 --> 00:04:33.079
Julien Ducloy: And after, if we look at, next edge, the site preparation, and extraction, extraction, sorry, the risk, shifts, to operational technology.

25
00:04:33.080 --> 00:04:49.870
Julien Ducloy: The control system that, that do the, the, that help for earth-moving equipment, GPS, and fleet management systems. The attackers who gain access here can cause, direct physical disruption and create, safety hazards, for workers.

26
00:04:49.890 --> 00:04:50.570
Julien Ducloy: No.

27
00:04:51.110 --> 00:05:04.430
Raul Munoz: Yeah, I mean, safety, a huge one, and I guess that brings us to perhaps the next stage, which is processing. That's probably often one of the most complex systems within, I guess within the mining complex.

28
00:05:05.360 --> 00:05:20.950
Julien Ducloy: Yeah, exactly. Process would be, the highest, value target, and ransomware attacks on processing systems can help, production entirely. And sometimes for, like, minimum 4 days and weeks or months.

29
00:05:20.950 --> 00:05:34.689
Julien Ducloy: And any disruption to a processing cover system then can compromise either the product quality, or create, physical damage, with, all-the-time significant, financial losses.

30
00:05:34.850 --> 00:05:44.619
Julien Ducloy: So, the combination at the stage of IT and OT exposure is… it becomes, particularly complex, to manage.

31
00:05:45.550 --> 00:06:04.590
Raul Munoz: Right, so we've gone from exploration to extraction to processing and some of the systems that could be affected. But even after the ore is extracted and processed, there are risks in transportation and commercial operations, right?

32
00:06:05.390 --> 00:06:20.729

Julien Ducloy: Yeah, transportation system is a great target, and stealing shipping information to disrupt logistics, create safety hazards, and steal the ore are still the final product. Those are, like, great targets for attackers.

33
00:06:20.730 --> 00:06:45.319
Julien Ducloy: When we think about marketing and general administration, then you fall into the classic, cyber risk, fraudulent wire transfers, and confidential competitive information, pricing, contract, customer data. So we can see overall that the, the attacks you face across the lifecycle is, quite broad, for many industries.

34
00:06:46.590 --> 00:06:59.990
Raul Munoz: So with all that broad range of exposures across the lifecycle, how should mining leaders begin to build meaningful resilience within their organization?

35
00:07:01.460 --> 00:07:18.200
Julien Ducloy: So, you start with, like, the identification. They need to understand their specific risk profile. So, what is the infrastructure, what are the most valuable assets, and where are the security gaps and the vulnerabilities?

36
00:07:18.200 --> 00:07:26.760
Julien Ducloy: So, and then, at the end, when we look at combining the asset and the security gaps, what is the potential financial impact of an incident?

37
00:07:26.760 --> 00:07:44.390
Julien Ducloy: So, you can't protect, everything equally, so you want to prioritize, and, for that, financial, impact quantification is, critical, and, it's what gets you the attention of, management level, from management level.

38
00:07:45.960 --> 00:07:56.370
Raul Munoz: Right? Now, the guide goes into, you know, very, into a lot of detail, when it comes to cyber hygiene control, specifically 12 of them.

39
00:07:56.480 --> 00:08:03.470

Raul Munoz: Could you perhaps highlight, what you think are some of the most critical steps and hygiene controls?

40
00:08:04.300 --> 00:08:09.659
Julien Ducloy: Sure, and I'll try to not to be too technical, but some of the

41
00:08:12.180 --> 00:08:35.419
Julien Ducloy: Yeah, well, I guess some of the work will resonate with, like, everyone, like, multi-factor authentication. I think at this stage, everyone has heard about that, so this is… this is because this, control is foundational, it's the single most important, control, and because it prevents, unauthorized access, like any, like no other control would do.

42
00:08:35.419 --> 00:08:47.919
Julien Ducloy: Now, also, a very well-known control is endpoint detection and response, because it would help to both identify the threat directly on systems, but also start to contain it.

43
00:08:48.640 --> 00:09:02.780
Julien Ducloy: And if we look at the other end of the, spectrum, after a problem has happened, secured and tested backups. So that's, absolutely critical, is what generally is, like, your last.

44
00:09:02.780 --> 00:09:13.730
Julien Ducloy: the last thing that prevents you from paying a ransom, potentially. And so it's not about just having backups, but also regularly testing whether we can actually restore from them.

45
00:09:13.730 --> 00:09:19.790
Julien Ducloy: And how efficient that is. And last, I will mention patch and vulnerability management.

46
00:09:19.790 --> 00:09:36.110
Julien Ducloy: Keeping systems up-to-date is basic, but it's difficult, and, because of all the production constraints, and, it's often where attackers, find their way, through the systems with, like, the un-patch one.

47
00:09:36.440 --> 00:09:37.380

Julien Ducloy: And,

48
00:09:37.380 --> 00:09:56.729
Julien Ducloy: This part is actually getting worse, with the powerful cyber-capable AI models. So that's something that's right now in the, really, in the heart of the discussion on security improvement, due to, the latest AI capabilities on cyber.

49
00:09:57.030 --> 00:10:01.140
Raul Munoz: Yeah, it's incredible the speed at which… at which that's developing.

50
00:10:01.240 --> 00:10:15.509
Raul Munoz: Now there's, we are at a phase where this isn't just an IT problem, and that's when this becomes an enterprise policy dimension, isn't it?

51
00:10:16.670 --> 00:10:33.939
Julien Ducloy: Yeah, this is really important, like, we have been seeing that for 5 or 10 years now, and I think organizations get it now, but cyber resilience requires buying from every department. Operations, HR, finance, legal, and the C-suite.

52
00:10:33.940 --> 00:10:56.520
Julien Ducloy: enterprise-wide policy would define roles and responsibilities for every team, and those policies need to be operationalized through regular training, and with a strong coordination between IT and OT security. That's really key, because attackers would… otherwise, they slip through the cracks, between IT and OT. That's what we see.

53
00:10:56.540 --> 00:11:11.640
Julien Ducloy: For example, a phishing test that, an employee fails, is a learning opportunity for him, but a phishing attack on an untrained employee, that, for which he falls for, it's a potential crisis.

54
00:11:12.820 --> 00:11:15.600
Raul Munoz: Yeah, no, all quite critical

55
00:11:15.800 --> 00:11:24.800
Raul Munoz: All right, to close, one final thought on cyber risk to our listeners in the mining sector. What would you like to say?

56
00:11:25.790 --> 00:11:26.750
Julien Ducloy: Productivity.

57
00:11:27.830 --> 00:11:37.229
Julien Ducloy: Minor organizations, they are uniquely vulnerable, because they combine high-value data, complex operational technology, and often they have

58
00:11:37.230 --> 00:11:55.419
Julien Ducloy: older legacy systems that are difficult to patch. So they cannot wait for a cyber incident to start building their resilience. They need to cover, basics and control already in place. And especially something we haven't mentioned yet, but an incident response plan documented

59
00:11:55.420 --> 00:12:06.640
Julien Ducloy: and practiced. And, and so they can understand, as a group, the potential financial implications, before they need to explain them to investors, which in the worst case.

60
00:12:07.890 --> 00:12:27.730
Raul Munoz: Yeah, thank you very much, Julian. This is a really important conversation, and as you suggested earlier, one that's becoming a lot more critical with some of the advancements in technology. Really appreciate your insights. A reminder to our viewers, the Resilience Guide is available on marsh.com.

61
00:12:27.940 --> 00:12:47.410
Raul Munoz: And in our next and final episode, we shift to a challenge that's probably top of mind with everyone in every sector, but particularly in the mining industry, and that's your people. So I hope you join us next. Thank you, Dave. Thank you, Julian, and we'll see you next.