Lowenstein Sandler's Insurance Recovery Podcast: Don’t Take No For An Answer

Episode 96: Cyber Insurance for Operational Technology: Where Computers Touch the Real World

By Lynda A. Bennett, David Anderson

OCTOBER 2024

Lynda Bennett: Welcome to the Lowenstein Sandler podcast series. I'm Lynda Bennett, Chair of the Insurance Recovery Group at Lowenstein Sandler. Before we begin, please take a moment to subscribe to our podcast series at lowenstein.com/podcasts. Or find us on Amazon Music, Apple Podcasts, Audible, iHeartRadio, Spotify, Soundcloud or YouTube. Now let's take a listen.

Lynda Bennett: Welcome to Don't Take No For an Answer. I'm your host, Lynda Bennett, chair of Lowenstein Sandler's Insurance Recovery Group. Today I'm very pleased to be joined by David Anderson, who's a Vice President of Cyber at Woodruff Sawyer. Welcome, Dave. Glad to have you back.

David Anderson: Thanks for having me back, Lynda. I feel like we haven't done this in a minute. So good to be back in a hot seat.

Lynda Bennett: Well, I'm glad to have you back to talk about a very important topic that really doesn't get enough attention as we talk about cyber insurance, and that is the risks that are associated with operational technology. Over the last several years, there's been a ton of discussion around cyber-attacks and their impacts on companies' information systems, aka IT systems, but it's just as important for businesses to understand the risks associated with their operational technologies or OT systems. So Dave, why don't we start by having you tell us about what are the differences between IT systems and OT systems, and how common is it for businesses to face a cyber-attack or other cyber event on their OT systems?

David Anderson: Yeah, Lynda, happy to. I think that's the best place to start because this is often not thought about when people are buying coverage. IT systems or information technology systems are really the computer systems that you have to store customer data, your accounting, operations, even the laptop that you use, Lynda, on a daily basis to help your clients out, that's all considered IT. It's information technology, it's a means to access information.

Operational technology is a pretty large umbrella catch-all name if you want to call it that but can include specific systems like building management systems for real estate and property managers, industrial control systems for HVAC, oil pipeline, et cetera, that controls valves and pressure gauges, et cetera. Or SCADA, which is, I don't remember what the acronym stands for, but it's definitely a well-known operational technology system and basically the difference between IT and OT is OT uses a computer to interact with the physical world. It's doing something for you, it's making something for you, it's storing something for you at a specific temperature or humidity, and so I think the simplest delineation between IT and OT is that OT touches the real world.

Lynda Bennett: Got you. Now, there are some risks associated with cyber-attacks. What are some of the risks that are associated with cyber-attacks on OT systems? It sounds like we have a couple of different buckets of types of loss that companies could experience, so why don't we cover those?

David Anderson: If you could imagine a Venn diagram of IT risk and OT risk, there are several commonalities between those two types of systems. You still have the risk of a ransomware attacker or even a fat-finger system failure event, either disrupting the operational technology machine itself, messing up its source code. It can get a virus just like your laptop can. It's still fundamentally computer with a processor and memory that just runs through lines of code. But instead of putting a PowerPoint together, it moves a little arm that fastens the door to your car when it's in manufacturing stages. So you have traditional network interruption exposures in so much that a malicious event or a system failure can bring down your operational technology systems. You have the same sort of restoration and reprogramming costs that you might otherwise face in regular server or laptop if it was wiped or if the data or operating system was corrupted.

The unique risk for operational technology versus information technology is the consequences of those machines going down. So you have pretty basic operational technology if you have a smart thermostat in your house, and then there's very sophisticated operational technology that puts together the wafers for microchips that deals in margins of error, 1/1000th of human hair. And so if you have a corruption in the programming, malicious or non-malicious, if you have a network event that brings down the ability for those operational technology components to communicate and do their job, the consequences of that then impact real-world things, whether it's raw material, temperature sensitive material, building management, things like escalators, elevators, heaters, etc. That's really where the risk is different. You have a computer system, fundamentally, it's still a computer system that's been brought down, but instead of just getting the blue screen of death and taking the day off while IT fixes it, you've got $2 million of raw beef that can't be processed sitting on the assembly line.

Lynda Bennett: Right. I'm going to zoom out and think about if I'm the CEO of a company, what is the OT risk that's keeping me up at night? It falls into the three buckets of financial risks. So you go down, you've got business interruption, you've got wasting inventory, as you just said, of our beef. We also have safety risks. So when the escalator suddenly abruptly stops and somebody goes falling down those stairs, we've got risk of physical injury for people that are in those facilities when you have that failure. And then of course we have the physical damage. So one of the things that I've thought about are these pipelines that now use this or that can unexpectedly release materials into places, right? So we've got physical damage that can happen. So financial risk, safety risk, physical damage risk. So Dave, tell us about what cyber insurance is available for that. Can we get a one-stop shop insurance policy or do we have to create our patchwork quilt again of insurance to get everything covered there?

David Anderson: Well, as is a common theme on Don't Take No, the answer is the coverage matters and the terms and conditions and definitions matter as it turn out. So any broker that works with our clients on cyber risk policies needs to fundamentally understand the operations of the business. So I think it's a pretty safe guess to say Lowenstein Sandler and Woodruff Sawyer don't really have any operational risk, but if I'm dealing with either a large industrial conglomerate or a healthcare distributor or someone who's in the food processing business anywhere in that sort of supply chain, to be fair, you really need to get an understanding of where computers touch the real world.

And then once you've looked at that, then you need to look at your cyber insurance policy and see if the policy dovetails. Not every cyber insurance policy, Lynda, affirmatively contemplates operational technology components or systems within the definition of an insured computer system. And more importantly, the bricking insuring agreement, which steps in to replace computer hardware if it's rendered permanently useless oftentimes will either explicitly include operational technology, explicitly exclude operational technology or is silent.

So unfortunately, the answer is it depends. It really sort of matters when you look at whether or not these few crucial definitions within any cyber insurance policy and the bodily injury property damage exclusion within the cyber insurance policy are trying to affirmatively grant cover for OT, are trying to clearly exclude it or are silent. And our listeners know this, cyber insurance policies are incredibly disparate, and so it's just important to note that not every policy is a good fit for every insured, and you should be able to discern that. It's the same as buying a car. If I'm going to go off-roading in the Rockies, I'm not going to roll up in a three series convertible. I'm going to get a pickup truck. And so they're both great cars, but they have their specific use cases and it's important you look at the definitions within the policy to understand if this insurance company and the wording itself is trying to cover operational technology risk or not.

Lynda Bennett: Well, and ideally that's something that you're going to be doing, the companies are going to be doing at the front end, at the purchase phase. I usually hear from people after they've got the unexpected surprise that their coverage isn't what they thought it was after a claim has been presented. But as you and I, Dave, both know, we've worked together on matters regularly, it is a much better practice for companies to read and understand the policies that they're buying on the front end.

As you said, these policies are the wild west. The terms and conditions vary greatly across the market right now, and as I tell my clients, hope is not a great strategy. I would rather read the policy, say, hey, this doesn't explicitly provide coverage for OT that's not specifically identified in these very crucial definitions that will trigger coverage. And so it's far better to have that knowledge, understanding and importantly that conversation before the policy is bound rather than trying to address the silence of the issue and convincing a court that of course, that's what we reasonably expected and understood was going to be the case. Get clarity on the front end.

David Anderson: And sometimes you can just get an endorsement that just enhances the definitions. Like it might just be sitting in the underwriter’s manila folder, and you just got to ask for it, right? So it isn't really that big of a lift, but I know you want to go into the weeds a little bit more, so I'll keep going.

Lynda Bennett: Yes, I do want to talk about once we've got the policy written the right way and we've got that explicit OT coverage, I do want you to talk a bit about the business interruption and extra expenses. How does that work particularly when my OT system goes down?

David Anderson: Yeah. This is where I think we're going to ask the listener for their forgiveness because we're going into the weeds, we're going into the cattails at this point, the weeds are so high. The cyber policy will cover 50 to 75% of the operational technology cyber risk that you want to address. It should cover the reprogramming costs. It should cover the bricking costs, again, to your point, if we have the right policy.

The question is do you have enough limit? And likely the property damage exclusion on the cyber policy will kick in as soon as we've stopped repairing operational technology, in other words, computer components which are generally insured under cyber policy and the exclusion kicks in when it's the buildings, when it's the raw materials, when it's the unfinished goods and stock throughput. And so the cyber policy should cover the resulting business interruption and extra expense and restoration costs associated with an operational technology outage.

The cyber insurance policy, again, if properly crafted, should cover the replacement costs of operational technology components if they're rendered useless. No traditional cyber policy, and we can get into what that means in a minute. No traditional cyber policy will cover the resulting physical damage that might happen to your property or goods, and there might be some grayness around the resulting business interruption or as our friends of property call it time element. If that business interruption, then ends on the OT side back online, but you've got three weeks now before your raw materials can be ready to process and put in your little box and put on the UPS truck again.

Lynda Bennett: Yeah, this is where insurance gets incredibly complicated. It's why you and I-

David Anderson: A little.

Lynda Bennett: Love what we do. It is a jigsaw puzzle, and all of the pieces need to interlock together correctly. And obviously our listeners fully understand based on today's episode as well as the ones that you've been on prior, that you need to have a super qualified and knowledgeable insurance broker. Shameless plug for Mr. David Anderson.

David Anderson: I'll take it. Thank you.

Lynda Bennett: But you're talking David about now the intersection of the whole coverage program here. So as you said, the cyber policy's going to take you 50, maybe 60% of the way there. So let's talk about what are the other policies that need to be considered noticed in the event of a claim, and then how do we put this jigsaw puzzle together to have a beautiful picture of full coverage at the end for the claim?

David Anderson: Can I counter you counselor by saying, let's talk about how we think about the program first and then think about how we deal with it in the claim?

Lynda Bennett: You bet.

David Anderson: Because I think that's a more logical workflow. So for those of you that are insurance brokers sneaking on this podcast, you can turn it off now because I'm going to give away some secrets. Everyone else is welcome to stay. Really what you need to do is do some sort of gap analysis on your entire portfolio of coverage. Let's just take a food processing enterprise as an example. Okay, we're 60% there on the cyber coverage. We know what it's covering there. We know that it's not covering the raw materials, the uncooked foods, the temperature as of nature. We know that it's not covering bodily injury health risks arising out of contamination or improper preparation. And so we've got the sort of basic cyber basis covered here. Then we need to look at what is your property policy covering. I can guarantee you that either your property policy fully excludes any perils, including time element or business interruption arising out of a malicious cyber-attack.

Sometimes a leave-in excluded out of a fat finger system failure event. We know for a fact that the product, most property policies don't even cover some sort of product recall or stock throughput is increasingly not covered under a property policy arising out of any peril, let alone cyber, right?

Lynda Bennett: Right.

David Anderson: So you need to understand where your lost drivers can be in the real world arising out of a cyber event, and then make sure that the policies that dovetail or fit in like a puzzle piece are where you can rely on. Most product recall policies do not have a cyber related exclusion. So if you had a cyber-attack that spoiled something, you're okay. Stock throughput, depending on where you buy it, may or may not have a cyber exclusion, but there's generally a buyback and surprise, it's not that expensive or hard to get in the grand scheme of things. The casualty policy, which also generally doesn't cover product recall anymore these days, should still cover the bodily injury of your facilities and your employees arising out of cyber-attack. But that stops at invasion of privacy because that's where the cyber covers it. So there's a number of different policies that you need to think about.

If you have an assembly line, a manufacturing line, a processing line that is run by a bunch of machines that need to be appropriately tweaked, endorsed, or enhanced to make sure that if a cyber-attack were to impact temperature sensitive pharmaceutical compounds, or maybe you're treating water like that story in Florida or making beverages in automated fashion, someone can come in and tweak that. None of that is going to be covered under the cyber policy. None of it's going to be covered on the property policy. It might be a product recall, it might be some other sort of distribution related to prices coverage, but you need to understand that. And so that's where you know to point to in the event of a claim, because you've done the gap analysis, you know where each bucket of loss arising out of that cyber-attack fits, and you have contract certainty instead of hoping on silence to address those losses. And the market, Lynda, is actually trying to be more deliberate about this in terms of offering products that are specifically suited for cyber physical damage exposures.

Lynda Bennett: All right, Dave, well, this has been fantastic. We are just about out of time and as usual, you have been not only knowledgeable, but incredibly engaging and fun to have on the podcast. I want to wrap it up for our listeners. One, you obviously need a very qualified broker like Mr. Anderson to help navigate this incredibly complex web of getting coverage for OT systems under both your cyber policies and under your traditional policies. I'm duty bound on Don't Take No for an Answer to say that in the event that you do have a claim, you need to notice broadly, early, often, and carefully look at the coverage position letters to try to put that puzzle together to make that beautiful picture of full coverage for the claim. But thank you, Dave, for coming on. As always, it is a pleasure to have you and we look forward to having you come on back soon.

David Anderson: Thanks for having me, Lynda, and talk to you later, Team Lowenstein.

Lynda Bennett: Thank you for listening to today's episode. Please subscribe to our podcast series at lowenstein.com/podcasts. Or find us on Amazon Music, Apple Podcasts, Audible, iHeart Radio, Spotify, SoundCloud, or YouTube.

Lowenstein Sandler's podcast series is presented by Lowenstein Sandler and cannot be copied or rebroadcast without consent. The information provided is intended for a general audience and is not considered legal advice or a substitute for the advice of counsel. Prior results do not guarantee a similar outcome. Content reflects the personal views and opinions of the participants. No attorney client relationship is being created by this podcast. All rights are reserved.