MARSH

Powered by Marsh FINPRO

Episode 11

Navigating the Evolving Cyber Risk Landscape in Energy and Power Amid the Energy Transition

Sarah Baldys:

Welcome to Powered, where we talk with experts on the front lines of the energy transition to understand what's changing, what's at stake, and what boards and executives need to know now. From emerging technologies to evolving liability exposures, our guests bring sharp insight into how companies can lead confidently through the energy transition. I'm Sarah Baldys, US power and renewables leader at Marsh's financial and professional liability practice, and I am thrilled to hand things over to your host, Grace Brighter.

Grace Brighter:

Gabe [DiGiamberadino] is currently a member of Marsh’s cyber team. His responsibilities include working with clients and prospects to help them understand, measure, and manage their cyber risk. Gabe’s responsibilities include presenting renewal strategies and analytics to clients, soliciting coverage from markets, and executing successful insurance renewals for clients. Gabe also serves as the energy and power cyber industry specialist nationally for the cyber practice.

Grace Brighter:

All right.
Hey, Gabe, thanks for being here today.

Gabe DiGiamberadino:

Thanks for having me. Happy to be here.

Grace Brighter:

So Gabe, as you look at the current landscape, what are some of the most pressing cyber risk challenges facing energy and power companies today?

Gabe DiGiamberadino:

Yeah, great question. Some of the key risks we're seeing or key exposures. Obviously, you see it in the news every day. It would be ransomware or at least the threat of ransomware and the impact that can have on a business, the concerns around downtime. Obviously, supply chain events are a pretty prevalent thing we've been seeing. So those incidents you hear about from a vendor, some supply chain partner, typically we see this from a technology company where then you're having that third-party impact from them suffering a cyber event, whether that's data breach-wise, impact to operations, et cetera.
Other than that, I mean, those are two of the more common events we've been seeing from a frequency perspective. But as we go into 2026, see the landscape of risk continue to change, we're seeing that with more digitalization of operational technology that can certainly increase the attack surface, lead to potentially more frequency of events, and potentially even severity, and certainly opens the door for these physical damage type of events. The ensuing damage that follows from a cyber event, and questions around what's going to be covered under a property policy, and what solutions exist in the cyber market to either bridge that gap or affirmatively provide cover.

Grace Brighter:

Great. That's awesome, Gabe. I think you already got into this, and most people maybe listening are aware of ransomware attacks and supply chain attacks. And those events definitely have significant impacts on utilities and renewables because of their essential roles in energy production and energy distribution. Just curious how these specific types of attacks differ in our industry compared to other industries.

Gabe DiGiamberadino:

Absolutely. I think taking a step back, what we've seen, at least with our data, is that generally, frequency-wise, there's been much lower frequency of events within this industry sector compared to other industries. Now, it's not to say that these events aren't happening and they're not important items to ensure against it and be mindful of and work to protect, but it is something we've been seeing less frequently. Now, that's certainly something that can shift. I think in a recent time, we've been seeing a little bit more of an increase in ransomware activity and a shift towards what we call low downtime industries.

Something like a manufacturing and energy and power sector because, lately, less and less clients have actually been paying ransoms when these events are occurring. In an effort to incentivize payment or try and get some funds because, I mean, at the end of it, threat actors are motivated by money. In an effort to incentivize payment targeting these industries that would have more concerns and issues with downtime, they'd be looking to target these industries and hopefully get some payment there. That's certainly one of it. I think, again, as there is more focus, or reliance, I should say, on technology and your technology providers, it's important to have a strong plan in place on vendor risk management.

For when these supply chain events do happen, maybe you have some level of defense and depth, some way to maybe mitigate to some extent some of that impact to your operations.

Grace Brighter:

Specifically thinking about energy and power, we know that cyber risk isn't uniform across the sector at all. I definitely want to get into how risk and exposure differs between the various segments within our industry, like renewables versus investor-owned utilities. I'm sure operational technologies present vulnerabilities in all of these sectors, but you mentioned things like attack surface. Just curious how maybe the unique characteristics of a renewable presents various risks that maybe don't exist with a big, owned utility.

Gabe DiGiamberadino:

Absolutely. I'd say broadly or generally speaking, I mean, the core exposures are going to be the same. Business interruption and ransomware are probably going to be the two items that really come to mind the most. There will be some small differences between each subsector. For example, with a utility, you're going to have more PII, more personally identifiable information, than some other subsectors. There is some level of a privacy exposure there, and maybe it's not the largest of concerns, but it still presents itself.
And then similarly, from a business interruption perspective, some of this loss from downtime, or I should say impact from downtime following a cyber event, may present as deferred revenue rather than actual lost income. For a utility, they may not have the same actual impact business interruption-wise for loss income. Obviously, they would still have extra expenses incurred, but that's one variation. But I think the biggest thing is just when we're looking less at subsectors, but more so at the range of size of the organizations and the resources that they have.

A large investor in utility or personnel dedicated to cybersecurity and the ability to invest more in their overall cybersecurity posture, whereas a much smaller organization, like a small renewables company, will not have the same luxury. Thinking in the event or the impact of a cyber event, it's going to be much more impactful to that smaller organization, relatively speaking.

Grace Brighter:

Great. Thanks, Gabe. Really appreciate you outlining some of those differences there. I think here, we can jump into the key concepts of cyber insurance. Obviously, cyber is such a hot topic right now. For many leaders, cyber insurance can be very complex. Are you just able to break down the core concepts as it relates to cyber insurance? What do companies really need to understand about the coverage that they have?

Gabe DiGiamberadino:

Yeah. The high-level overview is that the cyber policy is designed to cover financial loss that ensues following from a cyber event. Now, cyber event can be broad and could mean a number of different things, but the way I like to break it down is that within the cyber policy, as opposed to some other types of insurance policies, you have both first and third-party coverage. First party being directly incurred by the organization, third party, some third party was harmed or has some damages as a result of the cyber event that you had, and is making a claim against you.

Both of those within the same policy, and it's designed to be relatively broad, where it'll cover from discovery of the incident on a first-party perspective, your breach response costs, cost to engage with your legal counsel, help advise you what to do, what your notification obligations are, a computer forensics firm to help identify what the source and scope of the incident is, hiring a public relations firm, et cetera. You also have your data restoration and recovery costs, cost to restore, recreate or repair impacted data or data assets, business interruption, extra expenses, ransomware that costs to negotiate with the threat actor, pay the ransom if it becomes necessary and other forensics.

And then from a third-party perspective, you have your network security and privacy liability. You have a data breach or some type of network incident, a third party then making that claim against you for your damages, whether that's failure to protect their personally identifiable information, failure to protect your network, et cetera. That's the high-level overview. I know I could probably go on and on about that but didn't want to go too long about that.

Grace Brighter:

No, you're right, Gabe. And it's definitely a lot for companies, and I'm sure it's a lot for your clients to understand because it is such a complex topic, and there's definitely a lot of growth in the area as well. Assuming every company and every client is going to have a unique risk management approach as it relates to their cyber insurance, but just generally speaking, how should companies be thinking about limits that they purchase on a cyber policy or maybe exclusions, just coverage in general?

Gabe DiGiamberadino:

Yeah. I mean, our way we like to approach it here is breaking it down from making this more circular. Starting it, how can we help you understand what your risk is? From there, you have a better idea of what your exposures are, what potential impacts there could be to your business. Then we like to find ways to measure what that risk is. Using benchmarking, our analytics, like our Blue[i], potentially even doing a financial stress test to get a stronger idea into what a loss could look like, and accompanying those two together to effectively have you manage the risk, that actual transfer of the risk to then purchase the policy.

A lot of this comes from the analytics like our benchmarking or our Blue[i] model, other data from our claims data center, and then some organizations within the industry, obviously, have some peer forums to discuss what they're buying and things of that nature now. From an exclusion’s perspective, you're really going to run into the same key items as the main exclusions. You certainly have ... I'd say that the most important or most prevalent ones being property damage and bodily injury. Those are two items that are not going to be covered under cyber policies.
Now there are cyber property damage solutions in the market, and especially as some property insurers are going to look less and less for their policy to be picking up damage from a cyber event, that's going to become more prevalent. You have war exclusions, which are certainly a very important item for clients in this industry sector, and weighing your different options for the war exclusions certainly plays a very significant role in the decision-making process for these clients, and it ends up being a key issue. Yeah, I'd say those are probably the two items.

Grace Brighter:

No, that's awesome, Gabe. You really answered my next question, which was just about assessing exposure to cyber threats. How can companies really evaluate cyber risk and exposure? I know you mentioned benchmarking. I'm aware that Marsh has its own risk assessment tool, which you can definitely provide a brief overview, if you're willing to, but really just curious if there's any specific frameworks that are particularly useful in the energy sector.

Gabe DiGiamberadino:

Yeah. I guess I'll start more broadly because I think as part of our Cyber Self-Assessment, the platform we utilize that really serves as the application and suite of tools that help us run the benchmarking, run other reports, a lot of that is tied to or built on the NIST framework, which applies, again, more broadly. Then there's other frameworks like the SANS ICS framework that would be a little bit more tailored towards industrial companies. You also have NERC CIP, which is going to be providing standards, more of a framework to identify and secure some critical assets, sorry, that would impact the supply of electricity. I'd say those probably being the most prevalent again. Yeah.

Grace Brighter:

Great. Now I think we have a clear understanding of the exposures out there and we identified a lot of the vulnerabilities that exist. I think now we can bring the conversation full circle and discuss what cyber solutions are typically available, broadly speaking, and then just for energy and power companies as well.

Gabe DiGiamberadino:

Yeah. I guess speaking within the sector, there's been much more capacity available and a much broader appetite increase in let's call it a little over a year now compared to how it historically has been, especially around the hard market. In terms of options or markets that exist for energy and power companies, you have your mutuals and you have your traditional or your commercial insurance carriers. Mutuals are obviously going to be member-owned, not for profit, whereas the traditional carriers, for profit.

Historically, the mutuals have made up much larger of a market share for these clients. But again, with the appetite and capacity broadening from a traditional market perspective, that has started to slightly shift. With that, as part of the broadening of capacity and appetite, more of these traditional markets have been offering or willing to offer industry-specific coverage enhancements, such as failure to supply, NERC CIP fines and penalties from a regulatory perspective, spot market cover, relighting expenses, which again would be table stakes for tailoring coverage to the specific client.

And then outside of that, again, trying to make this full circle, more and more insurance companies are offering some type of proactive or risk management services that are available to policyholders, whether that's in the form of a credit, in the form of discounted services like a tabletop or something like that, is becoming more prevalent. And I think if we bring it back to the difference in organizations, like a large investor and utility or a much smaller company, taking advantage of some of these resources that might be available within your cyber policy could help bridge the gap between what you may be able to have access to with your own resources.

Grace Brighter:

You mentioned a lot of the capacity out there that exists and the various insurance companies. Just thinking about from the perspective of some of these cyber underwriters, just curious what criteria they consider when they're assessing companies for cyber coverage. Are there common controls or risk management practices that potentially better risk profile or have a positive impact on things like pricing or just eligibility?

And then I guess conversely, any red flags that come to mind that maybe underwriters look out for?

Gabe DiGiamberadino:

As part of our process, we have what we call our 12 key controls. And that's really going to be the items you would really expect, multifactor authentication, having secure encrypted backups, your endpoint detection, incident response planning and testing, logging and monitoring. All of those traditional key controls would be really what is expected of clients in terms of securing or procuring cyber insurance, and then taking that another step further then because a lot of these organizations will have that operational technology or OT component environment, there's going to be very much more of a emphasis and scrutiny into those operational technology controls, whether that's segmentation between your IT and your OT environments, making sure that your incident response plan is applicable for operational technology, and really delving into that in conjunction with, again, those core cybersecurity controls.

As part of the underwriting process, that's what underwriters are going to be looking for. Having above average level of these controls is going to help in terms of flexibility on terms and pricing, but really that the core of it's going to be the baseline of insurability. But then you can have that broadened appetite, that additional flexibility, as it gets demonstrated in your underwriting call, your submission, et cetera, that you're going, I'd say, above and beyond or putting more of that investment in. I guess on the other end of that, conversely, if there's maybe a lack of controls there, while it traditionally is something that would inhibit you from being able to procure insurance, there are solutions that we can certainly offer for these clients that might not meet the baseline of insurability and would be able to still get them insurance, get them quotes while they work on the remediation or the implementation of some of these controls or deficiencies.

Grace Brighter:

On that same topic of underwriting and the underwriting process, just curious how insurers are thinking about a lot of these evolving technologies, whether that be AI, data centers, just emerging tech in general, I think it's important to just acknowledge some of the risks associated with the rise of AI and the expansion of a lot of these data centers. Really just curious, from your perspective, how these developments introduce new challenges within the space that we work in, the power and energy sector.

Gabe DiGiamberadino:

I think the one way to put it is that, at least with AI, it's not necessarily creating net new risks or risks that don't already exist, but it is certainly amplifying existing risks. So being mindful of that, not just for cyber, but the implications it could have across other lines, depending on what AI is being utilized for, it can certainly have implications amongst casualty and other lines. I think that's the thing is, one, understanding that it's not necessarily creating or it's not a new risk. It's not I'm trying to ensure against AI risk, it's AI amplifying that already existing risk.

If I were to have a social engineering incident leveraged with AI, it's not an AI attack, it's still a social engineering attack. I think making that distinction is helpful because from then, a policy-level perspective, it's still a cyber event. It's still something that we would look and expect to be covered under cyber policies. Now there are some insurance companies that are looking to make affirmative coverage grants or affirmative language around AI just for that avoidance of doubt, but it's still not changing the events itself. And I guess with that, it is something, though, that insurers are asking more questions about how you're utilizing AI, whether you're developing your own model, what the model's being trained on, et cetera. There's definitely more scrutiny, more attention paid towards it, but it's certainly not really a new risk, I guess, to answer the question.

Grace Brighter:

So, Gabe, it sounds like some of the concerns and the risks that exist in the cyber world, cyber insurance world, are similar to those that exist in the world of D&O. As cyber threats intensify and corporate governance grows more complex, this intersection between directors and officers' liability and cyber insurance has become increasingly relevant. I think there's a lot of ways we can make the connection between these two coverages. What jumps to my mind right away would be a potential cyber-related incident that results in some reputational damage, and then, consequently, market value is impacted, or shareholder confidence is impacted. I'm just curious, from your perspective, where you see this connection and then what you believe boards and leadership teams should be doing to mitigate this risk.

Gabe DiGiamberadino:

100%. No, I think that that's a great potential example. And it could even be something as simple as not having those discussions internally, not engaging the stakeholders, maybe then failing to carry or purchase cyber insurance, and then that in itself creates exposure. If you have a cyber incident and that causes significant financial damage, then that failure to really put much consideration to it could create exposure. Other than that, I mean, with public entities, obviously, you have the SEC notification obligations, not abiding by that creates an exposure there. I mean, in terms of what can boards and leadership really be doing is having those discussions with stakeholders and making sure that you're making that informed decision. It's one thing if you're choosing not to buy cyber, but did you have the right information to make that decision? Understanding that cyber is an enterprise issue, it certainly impacts all facets of the business and making sure that you, again, empower the necessary stakeholders, whether that's risk management, finance, legal, to go to the board and have these discussions and make sure that they have all the information they need again to understand, measure, manage, and respond to cyber risk.

Grace Brighter:

Thinking from the perspective of our clients, our energy and power companies, they also face regulatory pressures around cybersecurity. What are some key compliance requirements and how do they intersect with this whole idea of risk management and insurance?

Gabe DiGiamberadino:

I think the good thing is that it aligns relatively nicely. NERC CIP being probably the most prevalent, but those standards include items like categorizing the systems, management of the security controls, training of personnel, your actual physical security, and then items like incident response planning or reporting. A lot of that aligns and flows nicely into the controls and information that we would be looking for as part of or what would be reflected as part of applications or the underwriting process, and questions that should be getting asked to the client. It's not necessarily going to be new information. It's likely items that they're already probably aware of, to some extent.

I think, again, it ties that all together, and it does bring more awareness and, frankly, probably even gives some more comfort to these organizations that cyber insurers are looking for the same level of information that's being expected of them from a regulatory perspective.

Grace Brighter:

Well, Gabe, this has been a great conversation today. As we wrap up here, really just want to hear from you the three top pieces of advice you would give to leaders in energy and power companies about cyber risk today.

Gabe DiGiamberadino:

Yeah, absolutely. I mean, I'd say the risk landscape is going to continue to evolve, and especially as I mentioned about the OT systems and them continuing to be digitalized and homogenized, it's important to just be mindful of all that. And in terms of preparing for incidents if and when they do occur is really what can have a material impact on that potential severity is that incident response plan and tabletops for showing that you're prepared for when these incidents do occur. Outside of that, as the cyber market continues to mature and be a more efficient solution to transfer risk, there's going to be more capacity continuing to be available and understanding that it's not a one-size-fits-all approach. We can certainly find ways to tailor coverage and align with the exposures of the individual organization. Again, understanding that is certainly a key item.

And then I think lastly, tying back to the D&O and the board conversation is just continue to have those conversations, whether that's internally, externally. It's just really important for everybody, from cybersecurity, legal, risk management, finance to all be aligned. And don't be afraid to look to the insurance community for any insights. There's a lot of information available and out there. Again, I think it's just keeping that flow of conversation is really another key item.

Grace Brighter:

Great. Well, thank you so much for joining us, Gabe. I think if those listening heard anything, it's just about how complex cyber risk is, but obviously, with some of these proper controls and coverages in place, energy and power companies can protect themselves, and they can continue to power our world. So really appreciate the time.

Gabe DiGiamberadino:

Thanks for having me. This is great.

Grace Brighter:

That's all for this edition of Powered by Marsh FINPRO. We hope you enjoyed our discussion and thank you for listening. You can rate, review and subscribe to Powered by Marsh FINPRO on Spotify, apple Podcasts, or any other app you're using. You can also follow Marsh on LinkedIn or X. In addition to your podcast feed, you can find more episodes of Powered by Marsh FINPRO at www.marsh.com/poweredbypod and more insights from Marsh on our website, Marsh.com. Until next time, thanks for listening.