BofA Securities 2021 InsurTech Conference

Company Participants

- Josh MacDonald, Chief Underwriting Officer
- Philip Edmundson, Founder and Chief Executive Officer
- Tracie Grella, Global Head of Cyber Risk Insurance

Other Participants

- Joshua Shanker

Presentation

Joshua Shanker {BIO 21718992 <GO>}

And we're live. Thanks for joining us today. This is the panel on cyber risks at the first annual -- hopefully Annual Bank of America US InsurTech Conference. We're broadcasting live from One Bryant Park here at the Bank of America headquarters, New York City. Happy to be back in the office and this is a really great panel here on cyber risks.

I mean, we have three companies who are going to be participating in our panel and all of them are at very different stages of who there are at companies and what they do. I let them introduce their companies a little bit. But we have Tracie Grella, who is the Head of Global Cyber Risk at AIG. She's a 25-year AIG veteran, former Head of Professional Liability at AIG. Welcome Tracie, thank you for coming.

We have Phil Edmundson, who is the Founder and CEO of cyber specially underwriter for Corvus. He's got a long tenure in the insurance industry. His business, William Gallagher, he sold it to A. J. Gallagher. He was early tech stage -- early-stage tech investor in the InsurTech area with CoverWallet and Verifly.

We have Josh McDonald. He's a Chief Underwriter at cyber specialist Elpha Secure. He's been underwriting cyber claims for Chubb, for Beazley. And I mean, really, it's a great panel. Thank you all three for coming.

We're going to try and I guess do this in a little bit of alphabetical order I guess. Tracy, why don't you begin tell us a little about what you're doing in AIG. And then, we'll go out to each of you and then I'll start asking some questions.

Tracie Grella {BIO 19460769 <GO>}

Okay. Thank you, Josh. Thank you for having me here today. I'm Tracie Grella, I'm the Global Head of Cyber Risk at AIG. And in my role, I'm responsible for managing cyber

insurance, the cyber exposure across all of our product lines at AIG. So we're not only focused on the cyber insurance products, we sell, but also cyber risk that we have in other products, such as property and casualty and all of the other lines of AIG.

And we're firstly managing that risk and working with our clients to better understand their exposure, taking data that we have from all the trends and activity we have over the last two years and developing insights that we share with our clients to help them improve their cybersecurity risk. We've also been using a lot of external data in cyber underwriting and we use that data to help our clients identify vulnerabilities that are on their network or malware that's on their network, that gives rise to lots of on this policy and we work with that proactively to help them improve their security in that way to make them improve their risk profile.

So, we've been writing cyber insurance for over 20 years. We're a leading carrier in over 50 countries around the world and the cyber market is definitely dynamic. It's time of transition and we are playing an instrumental role in insurance industry as in helping improve the security of our organization.

Joshua Shanker {BIO 21718992 <GO>}

Thank you. Phil, tell us a little about what you're doing at Corvus?

Philip Edmundson {BIO 18065064 <GO>}

Hey. Thanks, Josh. It's pleasure to be here with you and the other panelists. I'm the CEO and Founder of Corvus Insurance. We're InsurTech company that broadly uses new types of data to predict and prevent commercial insurance claims and to deliver value to our stakeholders, and our stakeholders are our risk capital partners, our internal underwriters, our brokers and of course the policyholders. And while we work in a number of commercial insurance areas, cyber insurance is the most elegant expression of our overall market thesis.

And here, we use our proprietary software to ascertain insights into the IT security of organizations that we consider for our cyber insurance products. And we not only execute on that on our digital platform but that we call the CrowBar, but we also use that to deliver IT recommendations, IT security recommendations to our policyholders and alerts so that when bad things happen in the middle of the year, SolarWinds, Microsoft Exchange, our policyholders know what they can do to prevent vulnerabilities from being exploited because we understand the same view of their organizations that the cybercriminals hold. So love this conversation, great panelists. Thanks for inviting me.

Joshua Shanker {BIO 21718992 <GO>}

And Josh, tell us about Elpha Secure and what you're doing in the market?

Josh MacDonald

Sure, thanks, and happy to be on the panel, I appreciate the invitation. So, Elpha Secure is a new MGA, cyber MGA in InsurTech space. And I'm -- we came around and response to what's really been happening in the cyberspace for the past couple of years. I'm sure the audience is aware of how the cyber risk transfer market is evolving and responding to the past year. By now, mandating insurers have proper security hygiene in order to be insurable. So, at Elpha Secure, we took that to the next level by actually embedding a full suite of risk mitigation software into the risk transfer product. We have built a solution over the past couple of years to deliver the necessary tools for small business to mitigate cyber threats, tools such as multi-factor authentication, EDR, VPN and patching.

And also the resilience should an incident occur off-site encrypted, cloud backups, security operations center, and incident response. We deliver all these tools to the insured at bind giving insurer the full end-to-end solution for all of their cybersecurity and insurance needs. So think of Elpha really as progressive snapshot for auto, but we're also putting seatbelts, airbags and breaks in the car.

Questions And Answers

Q - Joshua Shanker {BIO 21718992 <GO>}

(Question And Answer)

Fantastic. So I have a bunch of questions and you don't have to get the answers right. This isn't a quiz, this is more explain to people how markets scale and how it works. The first question is, how big do we think the market is currently I guess, measured in premium of a big that may not be the right way to think about? How big could the market potentially be if everybody needed cyber risk, bought it and how should we think about it for municipalities and small businesses who might not be even aware that they need it right now? Can you sort of scale the market, Tracie, for us to give us a sense of what we're talking about here?

A - Tracie Grella {BIO 19460769 <GO>}

Yes. So there are lots of estimates about the size of the market. It's a little difficult to determine the actual size because of the way cyber exposure is embedded in multiple products. So it's not consistently captured from sources and from all industries across all companies the same way. Some companies may purchase some cyber risk and property or other lines, there is space in cyber insurance, there is package policies that include cyber. So we haven't really had an actual, an accurate measurement of what that number is. But it's definitely -- it's in the face all the different estimates that we have. It is a robust market and first ended -- there are offerings that applies to all size organizations. But small organizations can get package policy, so their cyber and it a lot of the services that were just being mentioned. You might find some sort of small companies, larger companies, the products available that more customized and can be a little bit more robust for larger companies.

So there's the market is pretty robust and able to address different size and to these different industries, but the actual size on a number is something that there's been a lot

of -- there's been different estimates on. But the more markets have been regularly coming in and at some point we have about 200 markets offering cyber insurance. So it is a robust and vibrant market.

Q - Joshua Shanker {BIO 21718992 <GO>}

Now, I'm just keep going through questions, although somebody feels like something's open-ended wants just type in, you can interrupt me, the more information we get the better. Can we talk a little about structuring, I guess? So some risks are small and a underwriter can take the whole risk themselves, other risks are large and requires syndication. I guess there's two things, I want to know a little about that market may be so you can do about syndicated market versus the whole market.

But the big question is people worries. Whenever I hear, there's a big loss in the cyber market that we assume it's part of the syndicated market. Is everybody on that loss? Is underwriting a tool where in the big syndicated deals, some companies are on, some companies are off? You talked about how I guess structural a little bit to understand what's going on?

A - Philip Edmundson {BIO 18065064 <GO>}

Josh, I'll give that a try and then I'll connect that to your first question as well, because I think this is more interesting color there. But you're right. Organizations are buying more insurance and frequently they need to use multiple insurers. Many insurers are reducing the amount of limit that they want to expose for any individual organizations. So, those are typically stacked up horizontally, frequently with the broadest coverage at the bottom and sometimes with restrictions on coverage as you go up a tower of insurance, but not always.

So -- but how that integrates into the earlier question, sure, we all read these estimates, maybe the U.S. market is $4 billion, maybe double that globally, great growth potential, but the interesting thing to me is how the growth is taking place, because not only our prices going up, premium rates going up, and that's driving growth, but demand is growing because organizations have much more awareness of cyber risk and as Tracie said, there's lots of cyber insurance available. And they're also -- so they're buying more than they did before and they're also requiring each other to buy more.

So frequently, organizations are required to buy certain types of liability insurance before a third party will do business with them, that could be a landlord-tenant relationship or a contractor-subcontractor relationship. Those requirements for cyber insurance didn't even exist five years ago. And now, they're increasing and so there's a second driver. And the third driver, let's face it and commercial insurance doesn't usually get a board level conversation. But what Board of Directors isn't talking about cyber risk today. They all are and their brokers will generally get dragged into the meeting and try to explain, why do we buy $5 million of insurance today?

And oftentimes, the next question is, how much does 10 cost and how much is 20 and the attention that's being paid to cyber risk is causing organizations to buy more insurance

because, there's frequently uncertain an answer to that question, how much is enough. So it's a lot of things driving the growth in the market and one way to answer that, are these horizontal towers of placements.

Q - Joshua Shanker {BIO 21718992 <GO>}

And for the smaller companies, I guess there's more risk flexion institutions that I want to know is, one is when there are large losses, is everybody on them? And the extent to which the market, I guess how big is the market -- is the market bigger for these large conglomerates and large corporations buying cyber or is it bigger for the many, many, many smaller entities who're buying little bits of protection each? I guess --

A - Tracie Grella {BIO 19460769 <GO>}

Yes, all carriers have -- there's a number of different underwriting processes, we even mentioned some of the things that we were doing as we opened up. And so carriers have different appetite right now and are targeting different types of business, whether it's small or larger industry based or control based on what they're looking for. So when you -- there will be many towers where not every company is on there. So much capacity on the market, there are many large losses out that large common carriers are not on those. You're not going to see that on every large tower, but every carrier is participating because there are so many markets that are available and because each market is looking for different type of risks and focusing their portfolio in different ways.

A - Josh MacDonald

Yes. To be back on what Tracie just said, there are some carriers whose strategy is only to place the primary and then maybe first or second excess. And then, some other carrier's strategy is to only place in high excess placements. So yes, there to peg back what you said, there are plenty of large losses where half of like the major carriers are probably not even on the loss.

Q - Joshua Shanker {BIO 21718992 <GO>}

And in terms of market right now, I guess, this is to Josh. I wonder if some of that is that stage of the markets in right now, at a stage where most players or some players are looking just to breakeven and learn about the debt that's necessary to become a great player. Are we at the stage where everyone's trying to make money? Is there a -- is this sort of -- is the whole industry in startup stage where the goal is just to be relevant?

A - Josh MacDonald

I think there is some partial merit to this view, really depending on the carrier. Up until, I'd say the past two years, most carriers were actually making money and pretty good money at that in cyber despite the relative infancy, there were ebbs and flows of profitability between major accounts in middle market and then various industry classes, but by and large those dynamics were manageable from a profitability perspective. Of course, there were some outliers who made some bad bets that didn't make money, but I believe that was the exception and not really the rule, but really that won't change in the past few years with the rising ransomware.

Middle market accounts which were historically a growth class quickly became unprofitable, but the problem is none of the carriers have the data to predict that quick turn and that's one of the issues with cyber risk, right? It evolves and changes quickly. Unfortunately to compound the problem, what we saw in the past five years was traditional incumbent carriers trying to achieve really aggressive new business goals, while competing with unsustainable rates in the marketplace, not similar to many lines across PNC, cyber was just a last line to get there. But most incumbent carriers at this point have largely taken like new business goals off the table this year and will be growing on rate alone while using their data to credit their books. Putting them, I believe, in a better position to return to profitability as opposed to newer entrants.

And certainly the carriers with the vast amounts of data will be in a better position to inform their underwriting and pricing moving forward and de-risk their book as much as possible. So I think that the view that you proposed has considerably more merit moving forward than it did historically.

Q - Joshua Shanker {BIO 21718992 <GO>}

Just to make a note, if you're listening to this webcast, you're probably accessed through the Vera cast web system, where although, we are not -- we're virtual and not live, it's possible for you to ask questions as well. You can take questions into the screen. I can ask them and I do -- well first, I have plenty of them, but if you have questions for me, please send them in and I can relay those questions.

So look, obviously, the claims are up due to ransomware and there might be some nervousness. I've often wondered what a real worst case scenario is for maybe a cyber theft event for the industry. I'm always worried about fat tails and things being priced, but escaping the perception. Tracie, to your estimation, is there something that I should think of as a cyber cat event where the industry sort of understands that this the major risk looming out there and is paying the price for that outcome?

A - Tracie Grella {BIO 19460769 <GO>}

The big concern for cyber insurers is systemic risk and that's what we've been focused on from the beginning of measuring the threat. So a lot of work goes into accumulation modeling and scenario development around the type of catastrophic event that we can have. Some of them could be a pass-failure type of vendor that is well rely on is industry that might have a vulnerability or some type of failure. And so, we -- all the carriers are working on developing those scenarios, sharing those scenarios and developing that model, right, A and B. The industry recently formed a consortium with a few carriers that are in that consortium now and hopefully more will be joining.

And one of the things that we're working on in that consortium is working together around modeling systemic risk and improving the data collection around that and we bring in suppliers, not only the key suppliers, but key cloud companies and others that are major aggregators so that we can better understand how they're managing their risk, what they see as the potential and make sure that we're working with onshore to capture the right data to measure that. So, that's an area of focus. It does need to continue to move

forward and develop, and there are some efforts with industry to work together to share all of our knowledge there to better model out that risk.

A - Josh MacDonald

I think just to add to that, Josh. As an industry, we definitely need better data and more granular data. We need to be able to have a full understanding of our insured security posture like down to the end point. That enables us to properly underwrite, and as important, that data enables the cat models, as Tracie mentioned, to more accurately measure those fat tails. But ultimately, that enables the industry to properly price the risk. When you think about not Petya, probably the closest we've come to a cat that easily could have been avoided for most companies if they had a proper patching in some place as Microsoft had released that patch for about three months prior to the event. So having insight into an insurance patching is just as an example, beyond the paper application is critical. If you're behind the firewall and you can see what their actual patching cadence is, then we can actually underwrite to that better and we'll have a more exact underwriting science than there what currently exists.

A - Philip Edmundson {BIO 18065064 <GO>}

Josh, this is really still a big, big challenge for the industry. Most of us assuming on the panel and others in this field look to a variety of third-party cat modeling companies and if you use multiple models, you'll find, at least, we have and we've heard from other competitors that you get very different results from these different modeling tools.

And so, I think it's fair to say there's not a consensus yet around what is the most likely catastrophe and then even if you can narrow it down that way, how do we model this, and some of the interesting developments that to look forward to are whether or not we see risk capital segmenting the risk and looking at this the way that the risk capital market looks at Florida Windstorm and says, well the very top catastrophic risk is something that we can pass off to insurance linked securities markets or other forms of capital as more and more tools, the tools we use and I think that Josh and Tracie use are able to score risk at the individual account level so that we can put together portfolios that are able to be at least partially securitized in risk transfer.

Q - Joshua Shanker {BIO 21718992 <GO>}

So I guess the answers sure are getting to my next question a little bit. If you look at this as a 20-year sort of line of business that was truly in its invitation 20 years ago, what were the initial data and variables that the industry was relying on -- early on in the process, what are contemporary variables and information that you're looking for and what will be as things are developing you're seeing, the emerging possibilities of things that are within the realm of knowable that are going to help refine the underwriting it for the next generation of products that are being sold?

I guess, Josh, why don't we start with you on that one? Or actually, I was still actually, sorry, you can't. Phil, so why don't you start there and of course Josh come in and Tracie. What is the data we're looking at, what was it, what is it, what will it be?

A - Philip Edmundson {BIO 18065064 <GO>}

The insurance industry over the course of my career, I have seen several new products emerge and get broad acceptance. And this is obviously one of those. The cyber risk started by as an outgrowth of professional liability of companies like AIG to Lloyd's of London, Chubb, other early pioneers who tried to use the smartest people in our business to build models for -- as Josh said earlier, for the most of this history, that model has led to an overpricing of risk and market that was not rational and produced above average profits until the last couple of years. Now, we're all focused on accumulation and catastrophe.

I think it's going to take some time for that to check out. I've spent my whole career at the intersection of technology and insurance. I'll use an example from another part of that career. We -- I have worked in the biotech sector in the 80s and 90s and at the beginning when biotech companies first started to bring drugs into clinical trials, commercial insurers charged a $1,000 per clinical trial subject for a $5 million insurance policy. Today, they charge about $10. So what happened there is at the beginning, there was a lot of fear and a lot of uncertainty and a lack of track record that led to an over pricing or over caution in pricing risk because everybody was afraid of biotech. Don't you remember, we used to have headlines about unmanageable fears of altering DNA.

And then, we all got used to it and things settled down. So it'll be interesting to see if cyber follows that same pattern or not. But right now, we've gone down a path where initially the industry overpriced risk. Now, the cybercriminals have taken the upper hand and we'll have to find a new equilibrium here in the coming years. I don't think it's going to be months, it's going to be years before it settles.

Q - Joshua Shanker {BIO 21718992 <GO>}

And then to understand the claim side of the equation. So I mean, in the past decade or so, some of the -- or maybe five years, some of the more -- some of the more notable events have been the Equifax data hack, the Kohl's data hack, the Colonial Pipeline hack. There is a combination of data privacy thievery. There was ransomware. Can we talk about a little bit, Josh, about the claims for nearly having private data stolen versus having a ransomware attack? There was this past year, a large insurer -- was major ransomware attack that was -- that costs a lot of money. As the claim -- the things are very different sizes that we referenced different situations. What does the claim specificity look like to help us understand what's at risk and try and come up with an understanding for the industry about -- what protections we're looking at?

A - Josh MacDonald

Yes, sure. So the Equifax incident, even in contrast to what we were seeing in the news of ransomware was still a massive loss, but the drivers of that loss were different. So notification and credit monitoring expenses and then forensics to determine the root cause and scope was what really drove that loss. As opposed to ransomware, which does require a heavy forensic response, it's usually the resulting ransom and business interruption that drives the loss. Before ransomware, as akin to the Equifax breach, personal information aggregation was the biggest exposure when underwriting the cyber risk. And so it was relatively easy to quantify the exposure to a certain degree, what are

the number of records? These could be credit card numbers or security numbers, et cetera. And while PII breaches can and do still occur, technology and controls have advanced to a degree where organizations can largely scope these exposures out of their risk profile. But what's difficult to price in this current loss environment is the unknown associated with ransomware. How much of the hacker is going to demand or how much of the hacker is going to demand? Can clients recover and restore in an efficient manner to avoid a lengthy business interruption?

But the good thing is, as we speak, all carriers are accumulating the data that will help better inform their underwriting questions and processes and pricing in response to ransomware. So that's really the evolution that we've seen from one threat vector of being or one threat being massive PII aggregation, which we still see to sort of the unknowns that we are facing with ransomware right now.

Q - Joshua Shanker {BIO 21718992 <GO>}

And is it -- is the rise in ransomware an outgrowth of crypto? Like, again, can ransomware exist without crypto?

A - Josh MacDonald

Well, it's a tough question. I think a lot of fingers are being pointed in that direction, and I think that there is certainly a degree of blame to be associated with crypto, but it's not all on the hands of crypto. I mean, there's certainly -- certain aspects that regulators can do with crypto, making it less transparent and easier to track criminals, and therefore, easier to get the funds back and/or prosecute those criminals. But there are other things that go into it, such as poor cybersecurity hygiene. I mean, as long as we implement a baseline of cybersecurity for companies that are doing business on the internet, that would prevent a lot of ransomware claims on its own. So there's a lot of different factors that go into it. But crypto certainly does play its part.

Q - Joshua Shanker {BIO 21718992 <GO>}

I'm going to pause for a second, because we have some questions from the audience. I have more questions, but I'll ask some of theirs. Can you make some comments about cyber reinsurance? Seems like that's much harder to price. Do you guys have any thoughts about the reinsurance markets for the audience? Anyone can answer.

A - Tracie Grella {BIO 19460769 <GO>}

I can't comment about the pricing of the reinsurance market, but the reinsurance market is certainly an important piece of the market for cyber. Many carriers are using reinsurance. And again, to use that, there's systemic risk exposure. So we're spreading the risk out, and so that is an important piece. And there is a lot of start-up companies coming in and offering cyber insurance. So they're relying on reinsurance as well. So it is a critical piece of the market. And the reinsurers are asking questions about systemic risk and how carriers are managing that, how we're collecting data, the data that we're capturing. And so they'll have an influence on that as well, what they see as important across from a systemic standpoint.

A - Josh MacDonald

Yes. I think, Tracie, you hit the nail on the head here. I mean, they really fear the aggregation. So capacity is starting to become tight and will probably be tight for a while to come. A lot of large primary carriers do rely heavily on quota share reinsurance. And so that pressure supply, I think, will really start to increase and continue for quite some time.

Q - Joshua Shanker {BIO 21718992 <GO>}

And the second question is while prices are up due to claims currently, have terms and conditions changed as well? Is -- can insurers buy the product they want? Is it available on the market? Or is -- or you can't even get, at this point, the amount of protection or the product you're looking for?

A - Philip Edmundson {BIO 18065064 <GO>}

Well, there are certainly exceptions, and there has been some tightening on terms, but not as broadly as there has been on pricing. So certainly, what not everyone realizes, I think, is that there's a lot of levers inside a cyber insurance policy. It's much more complex than most other types of commercial insurance policies. And so we're certainly seeing some of those knobs being turned down. But -- and in some classes of risk and companies that perhaps fail their IT security, scan tests or tools that we all use now, you may see some restrictions. But broad coverage is still available.

A - Tracie Grella {BIO 19460769 <GO>}

And a lot of the restrictions that are being introduced in the market are really incentive to help organizations improve their security. So you might see restrictions. But if a company can improve their security, we're giving guidance out, these types of controls that need to be in place, we're working with our clients to get those controls in place. We're identifying through scans and other data sources, we're identifying vulnerabilities and weaknesses. And when organizations can clean those up, then they will see more broad cover.

For those that can't or aren't investing now or something we hear a lot that this is a plan, but it does take time and it will be over the next couple of months, the next year, there will be restrictions on cover.

Q - Joshua Shanker {BIO 21718992 <GO>}

So when I think about ransomware, it triggers my head as an insurance guy that it somewhat relates to the old kidnap and ransom policies. And there was part of that which was the payment and protection for the buyer to pay those claims and get back their loved ones or whatever. But there was also a component of that a lot of these are specialists had black ops, former military personnel who would work to remediate the claim after payment and give the ransom back. To what extent are the claims departments for cyber risk underwriters involved in trying to minimize claims through remediation, through trying to, I guess, find who the villains are in this whole story and get the money back over time as a way of minimizing their own costs? And I guess I'll go to Tracie on that one.

A - Tracie Grella {BIO 19460769 <GO>}

Okay. There are a number of external vendors that are involved in this process. The claims department is certainly involved, but there are ransomware negotiators or vendors of cryptocurrency that holds cryptocurrency wallet and very -- and clients, the ransomware negotiators are working with law enforcement, the law firms are working with law enforcement. So there's a number of parties that are involved and then you have the private firm as well so -- and then there's others.

So the claims department is involved with -- working with these various vendors and certainly working with the insurers through this matter and helping to give a sight on how to recover in a most cost-effective way. But definitely a number of experts have to come and be involved in this type of negotiation and discussion.

Q - Joshua Shanker {BIO 21718992 <GO>}

So I think the latest news or latest big story was the JGB meat processing plant. Without betraying my own ignorance, that doesn't sound like the bedrock of cybersecurity that that target might have been able to be hackable before. It wasn't like a momentary letting down of the guard. I just imagine, there's a lot of hackable businesses out there. Are we at the trough of cybersecurity hygiene right now? Are -- as we go forward, is hygiene going to get a lot better and it's going to be harder to hack into various targets? Or is this kind of like code and semiconductors and Moore's law that as time goes on, well, silicon wafers get cheaper and thinner, the amount of code is doubling, so we're kind of running in place?

Will the hackers get more sophisticated at the same pace that cyber hygiene is improving? And so we're going to be at this equilibrium in -- for the foreseeable future? Phil, I guess I'll go with you on that question.

A - Philip Edmundson {BIO 18065064 <GO>}

Josh, that is a great question. And I think you got to the most difficult part at the end there, is, will the cyber hackers, the cyber criminals continue to grow in sophistication? Will they be able to continue to hide under the protection of certain governments or in other ways, a good law enforcement? Because they will need to ramp up their game, because so much is being spent on cybersecurity, not just because we recommend it to our policyholders, but organizations are doing this and investing broadly. Maybe not all of them, but broadly into cybersecurity. And I'm sure one of your colleagues that covers the cybersecurity software market can talk about that at great length.

So big challenges there and a lot of uncertainty about how the cyber criminals will be able to continue to stay steps ahead of the cybersecurity industry and those of us who underwrite the risk.

A - Josh MacDonald

Josh, I'd jump in there and say that I think the rule of thumb going to JGB is that any company can be hacked. That has been proven many times over. If you think about DNSA,

Mandiant, military agencies and the biggest banks have all been compromised. And they have the best cybersecurity in the world.

I'm not privy to JGB's network security, but it is known that manufacturing is a vulnerable class with outdated operational technology and a high dependency on uptime. So their control is going to be best-in-class. But when you have the power of a state-sponsored actor breaking down your door, very few companies stand a chance of prevention.

So in the context of ransomware, it's how resilient is a company when they're hacked? Could JGB recover their data quickly to avoid a substantial interruption to their operations? Did they have a business continuity plan in place? To your point that the hacks are still making news, making them appear infrequent. But I would estimate that probably less than 1% of hacking incidents actually make the news.

Hackers are taking every opportunity they can right now, because as you said, security hygiene is only going to improve across the board. Governments are demanding better hygiene, industry groups are demanding better hygiene, insurance carriers are now demanding better hygiene. And once the baseline of cybersecurity hygiene improves, because it was very low before, especially in the middle market to small, even a modest improvement across the board, I think, will make a significant impact.

Q - Joshua Shanker {BIO 21718992 <GO>}

I guess something that Phil said does tell about a relationship between cyber hackers and state sponsorship. To what extent are there going to be successful cyber hackers without the protection and funding of a state sponsored, a state as a bad actor being a funder, a sort of villainy and whatnot? Are many of these cyber hackers truly independent and just villains for their own purposes? Or is this necessarily tied to international peace disruption? I guess, I mean, -- I'll leave up to you. We're kind of out of order. I match this who is going to get to questions. Anyone can answer, just because it doesn't matter so much. But what's the linkage? We're going to go talk about terrorism a little bit. We're going to talk about flying a little bit. It can go anywhere. So you guys can take wherever you want.

A - Philip Edmundson {BIO 18065064 <GO>}

Yes. Josh, we rely on the reports from the FBI and the law enforcement agencies to answer that question. And that certainly points out the fact that in many cases, if not state-sponsored, there are state defenders of these attacks. But honestly, most of the events that we respond to, the party on the other side may have a code name, but they are otherwise pretty opaque and are mostly successful in staying that way.

Q - Joshua Shanker {BIO 21718992 <GO>}

So after September 11, 2001, the insurance industry had gummed up, because nobody wanted to -- no one really know how to price, really want to take the risk of a terrorist event becoming a property cat destruction for a lot of small -- risks large and small. And the federal government responded with TRIA as an umbrella protection that allow the insurance institute continue to underwrite without having to contemplate terrorists making

exactly. There's been no real claim under TRIA. I guess it's worked or it hasn't worked, but it's definitely been tested. But as we think about the ability of some of these cyber actors to potentially create mass havoc, where does criminality end and terrorism begin? And does the TRIA for cyber attacks does -- do we need a TRIA for cyber attacks? Where are we right now? And what do we have to contemplate? What fears should the government be assuaging with protection for the private market? Phil looks like he's ready to answer. So I'm just going to give to him. Anyone can answer.

A - Philip Edmundson {BIO 18065064 <GO>}

Yes, it's a great question, Josh. So my understanding is TRIA does not preclude cyber events from its definition of terrorism. However, the definition of what is an active terrorism has not been put to the test under TRIA. And there's a lot of different scenarios that could play out here where we have cyber criminals who, as I just said, are so opaque in their source and where there's not clarity around the motivations of their government sponsors, defenders or colleagues. So it is -- I think, what would be most helpful to the commercial insurance industry is clarity from the treasury department around when TRIA might respond to a large cyber event rather than the need for new legislation.

Q - Joshua Shanker {BIO 21718992 <GO>}

All right. And the final question, I guess, for today involves Mr.Biden and Mr.Putin. And so at the recent summit, Biden, I guess, drew a red line around 16 different sectors that the United States would not stand for any cyber hack disruptions. And I guess Mr.Biden believes that was within Mr.Putin's ability to limit the amount of cyber hacks.

When we think about how business is priced, did the cost of protecting -- should the cost of buying cyber insurance on those 16 areas go down, because presumably, they're under the explicit protection of the United States government in terms of prompting an international incident if something should happen? And does that mean everything else is fair game, and the price of the remaining sectors that were not specifically named, suddenly maybe should go up in value, because the United States have less of an aggressive view on what would be the response if something were to happen to those areas?

A - Josh MacDonald

My gut reaction to that would be, no. I mean, even if you scope Russia out, there's still several other state actors that would have no problem targeting those entities. So I don't think any insurance carrier would be prudent to place their pricing based on that loose agreement if even was an agreement as opposed to a directive.

A - Tracie Grella {BIO 19460769 <GO>}

If something changes, I mean, we always look at our portfolio based on different segments, where attacks are coming from, who their accounts and what the potential loss could be. So that would all -- we would address that. But you have to see that change, and it does seem like it would be unlikely, in agreement with what Josh was saying.

A - Philip Edmundson {BIO 18065064 <GO>}
Agreed.

Q - Joshua Shanker {BIO 21718992 <GO>}
So there's one question coming through here. And in a lot of different types of policies, acts of war are excluded. And if there is a cyber claim that was paid, and that later is determined to be the act of a foreign government who was actually the instigator of that attack, is that claim -- a claim that could be subrogated or could be -- to the government or whatnot? Is attack by a form of government a payable event? Or is that somehow excluded in how the business is underwritten today?

A - Tracie Grella {BIO 19460769 <GO>}
Typically, under any cyber insurance policy, there's not an exclusion for actors. So the actor who conducts the -- whether the actor supports that in itself is not an exclusion. So you do need to look at both war exclusion and other exclusions in the policy. And in the cyber marketplace, war exclusions were addressed years ago to make sure we know that many hacks come from state actors and state-sponsored actors. So in a cyber policy, that has been considered as a war exclusion. And there was some language that was removed.

But when you look at other insurance policies in the market, the war exclusion may be more robust and not written with cyber attacks in mind. So those who are concerned about having a cyber attack that might result in a property damage or some type of bodily injury, they are going to have a more strict war exclusion in those policies typically.

Q - Joshua Shanker {BIO 21718992 <GO>}
Well, thank you all for your time today. We are at the end of the session. I do appreciate you all joining. And if anyone has any questions for any of the participants, you can e-mail me those questions, and I can certainly pass them on to you. But it's certainly been interesting. And obviously, this is a topic that is constantly evolving. Best of luck to all three of you. And we'll continue the dialogue and learn more from each other as time goes on.

A - Josh MacDonald
Thanks for having us. (Multiple Speakers)

A - Philip Edmundson {BIO 18065064 <GO>}
Thanks.

Q - Joshua Shanker {BIO 21718992 <GO>}
And let's avoid those claims. All the best. Bye.