Autumn 2019

THE INSURANCE Insider

## TORONTO CYBER ROUNDTABLE 2019

# Call to arms

With more firms becoming aware of their likely cyber exposures, the battle is on to educate insureds about the magnitude of potential losses

www.insuranceinsider.com

In association with

Munich RE


## Let’s turn digital threats into client’s trust.

Find out more at munichre.com/cyber

NOT IF, BUT HOW

Munich RE

# Cyber surge

Dramatic headlines detailing data breaches and companies being hacked by criminals show little sign of going away, but despite these high-profile incidents, there is still some way to go before businesses truly come to terms with the cyber liability exposures they face.

Recent years have seen some of the largest companies in the world become increasingly attuned to the risks they face from cyber criminals or employees unwittingly (or knowingly) releasing data.

But gaps remain, and those holes in cyber risk management only seem to grow wider the more you move down the corporate food chain.

This issue, and many others, were discussed during a recent roundtable *The Insurance Insider* hosted in Toronto, Canada in partnership with Munich Re Syndicates.

While many companies do now understand they have an exposure to potential cyber losses, they do not necessarily understand the scale or magnitude of what those losses could be.

Indeed, few truly comprehend that what at first appears to be a fairly minor issue can in fact have a long-lasting, or devastating, impact on their ability to exist as a business.

And this, argued various members of the panel, can help drive the cyber insurance market's penetration in some of the more traditionally closed-off sectors such as the small-to-medium enterprise (SME) space.

But the hurdle, as has long been the case, is getting the message across to SMEs that the exposure they face is very real and that their business is very much at threat.

Sure, many SMEs may not store hundreds of thousands of people's private information, but they can find themselves locked out of data systems due to ransomware.

Some have speculated that the introduction of regulation such as GDPR in Europe or the NYDFS Cybersecurity Regulation in New York State would help spur the take-up of insurance products among SMEs. However, as the panellists noted, that has not necessarily been the case.

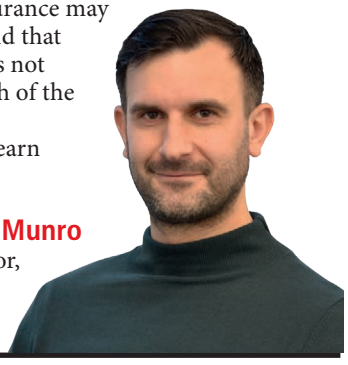
A rush into the market from all manner of insurance carriers means the sector is flooded with capacity. Consequently, there is a lot of competition, and rates for coverage are low. And this is in spite of the fact that there have been some major headline losses hitting the market.

Loss-impacted accounts will face price increases, but for the most part, the rapid growth of the market means that for those insureds that have not faced claims, the cost of coverage continues to reduce.

But cheap coverage does not necessarily mean it is good for the insured. An ill-informed buyer may just buy the cheapest product on the shelf without realising the vast number of exclusions within the policy.

When it comes to making a claim on the policy, the insurance may not pay out, and that ultimately does not help the growth of the market either.

Read on to learn more!



**Christopher Munro**
Associate Editor,
*The Insurance Insider*

## Participants

**Tom Allen**
Head of Cyber and Technology, Munich Re Syndicate Limited

**Angela Feudo**
Underwriter, Cyber and Financial & Specialty Lines, QBE Services Inc.

**Phillip Hoyt**
Consultant, Cyber Security and MGA Development Stage Companies

**Dmitri Kralik**
Underwriter, Ridge Canada Cyber Solutions

**Robert Parisi**
Managing Director, Marsh FINPRO

**Ruth Promislow**
Partner, Bennett Jones LLP

**Mike Senechal**
Partner, Boxx Insurance

**EDITOR-IN-CHIEF**
Adam McNestrie *adam@insuranceinsider.com*

**ACTING MANAGING EDITOR**
Catrin Shi *catrin.shi@insuranceinsider.com*

**EDITOR**
Laura Board *laura.board@insuranceinsider.com*

**FEATURES EDITOR**
Gavin Bradshaw *gavin.bradshaw@insuranceinsider.com*

**COMMERCIAL DIRECTOR**
Sajeeda Merali *sajeeda.merali@insuranceinsider.com*

**HEAD OF MARKETING SERVICES**
Benjamin Bracken *ben.bracken@insuranceinsider.com*

**HEAD OF STRATEGIC PARTNERSHIPS**
Oliver Nevill *oliver.nevill@insuranceinsider.com*

**SENIOR BUSINESS DEVELOPMENT MANAGER**
Baker Jaggwe *baker.jaggwe@insuranceinsider.com*

**SUBSCRIPTIONS DIRECTOR**
Tom Fletcher *tom.fletcher@insuranceinsider.com*

**SENIOR ACCOUNT MANAGER**
Georgia Macnamara
*georgia.macnamara@insuranceinsider.com*

**STRATEGIC ACCOUNT MANAGER**
Tom Lovell *thomas.lovell@insuranceinsider.com*

**SUBSCRIPTIONS ACCOUNT MANAGER**
Luis Ciriaco *luis.ciriaco@insuranceinsider.com*

**HEAD OF MARKETING & ANALYTICS**
Lynette Stewart *lynette.stewart@insuranceinsider.com*

**BRAND MARKETING & ANALYTICS MANAGER**
Aimee Fuller *aimee@insuranceinsider.com*

**EVENTS DIRECTOR**
Sara Donaldson *sara.donaldson@insuranceinsider.com*

**CONFERENCE PRODUCTION MANAGER**
Matthew Sime *matthew.sime@insuranceinsider.com*

**CONFERENCE PRODUCER**
Miraal Mayet *miraal.mayet@insuranceinsider.com*

**EVENTS OPERATIONS MANAGER**
Holly Dudden *holly.dudden@insuranceinsider.com*

**EVENTS MARKETING ASSISTANT**
Luke Kavanagh *luke.kavanagh@insuranceinsider.com*

**PRODUCTION EDITOR**
Ewan Harwood *ewan@insuranceinsider.com*

**SUB-EDITOR**
Steve Godson *steve.godson@insuranceinsider.com*

**JUNIOR SUB-EDITOR**
Simeon Pickup *simeon.pickup@insuranceinsider.com*

**SENIOR DESIGNER**
Mike Orodan *mike.orodan@insuranceinsider.com*

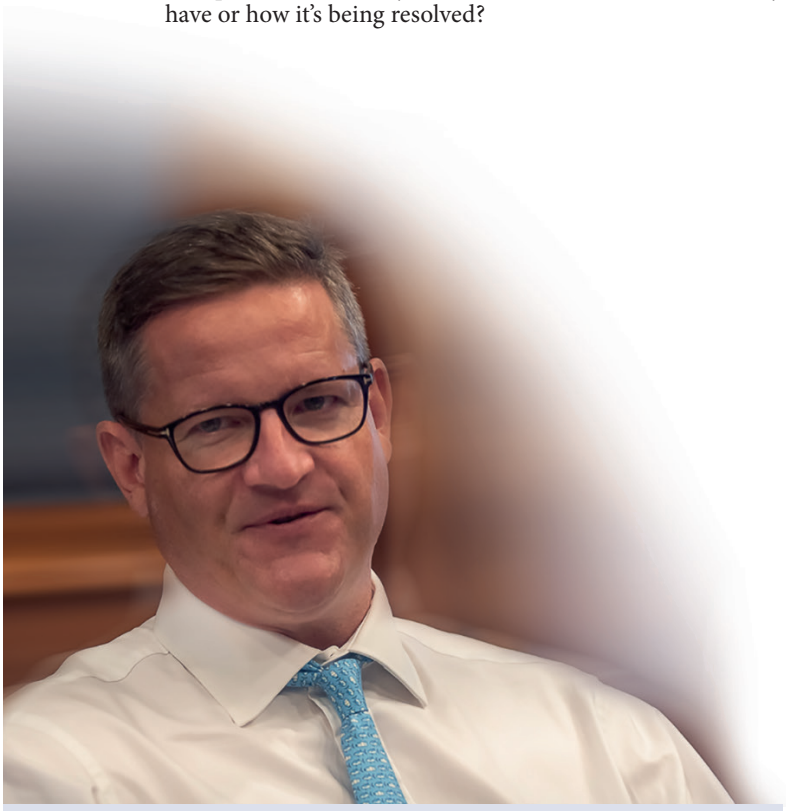
**Published by:** Euromoney Trading Limited, Level 1, 29 Ludgate Hill, London, EC4M 7NX, UK. **Tel Main:** +44 (0)20 7397 0615 **Editorial:** +44 (0)20 7397 0618
**Subscriptions:** +44 (0)20 7397 0619 **e-mail:** info@insuranceinsider.com. 

# Toronto Cyber Roundtable 2019

**Christopher Munro**
Are insureds still struggling to come to terms with the cyber exposure they face? What are your thoughts on that?

**Robert Parisi**
We've been working with Microsoft to get a better sense across industry and revenue classes as to where clients are in understanding their exposures, principally looking at whether they are quantifying their risk. That's usually indicative of whether or not they understand the risk.

You have a spectrum of some folks that are still in denial, but that's much less than it was. Now you've got to the point where most large companies, and even some medium-size companies, have CISOs [chief information security officers], which didn't exist 20 years ago. You have a risk that now has risen to the level of the board, so they know they have it. The question is, do they understand how much of a risk they have or how it's being resolved?



"Many industries such as manufacturing don't feel that data protection is really a front-and-centre risk"

**Tom Allen**

**Angela Feudo**
They do understand that there is an exposure but they don't quite understand how much these losses can actually end up costing. This can include forensic costs, the breach code costs, defence costs, ransoms etc. That's what some insureds don't have a complete grasp on yet.

**Christopher Munro**
There's sometimes a sense that it's mainly major corporations that are facing these exposures. Tom, what's your take on it?

**Tom Allen**
For certain types of industries the data protection aspect of the risk is very real. The product is tried and tested, in the sense that everyone has a pretty good idea of how they expect it to work, there are claims examples to point to and there's a lot of service provision available. There's a broad comfort zone amongst the buyers and sellers of this insurance in jurisdictions where this is seen as a real risk issue. This is a real product, it makes sense, it's got a track record, it's worth the money.

However, many industries such as manufacturing don't see themselves in that same context – they don't feel that data protection is really a front-and-centre risk. Cyber is a real risk for them, but the data protection product doesn't really mean that much to them and a lot of its covers are tangential. So I certainly get the impression that in industries where data protection is not really an articulated risk factor, outside of jurisdictions where data protection laws have been pretty clear, interest in the product drops off relatively quickly.

**Robert Parisi**
WannaCry and NotPetya made it real for a lot of people. Before, all you had to talk about was if you had a privacy breach. Then all of a sudden here was a major event that hit a variety of industries, causing massive business interruption and impacting the ability of the company to operate.

Overnight there were hundreds of millions, if not billions, of dollars of loss being pushed into the marketplace and it made it very real. And now you had real numbers, actual losses coming into the insurance market for business interruption from a ransomware, a technology-driven event that didn't have a physical component. And it's caused a lot of consternation in the marketplace.

**Ruth Promislow**
I can see that there is an increasing number of organisations looking to insurance as part of their solution. So you may take that as an indicator that they're understanding the risk. But at the same time, when I speak to them about basic

preparedness issues, I see an absence of an understanding of the risks.

So on the one hand they think "we have this risk, we'd better get this product, that will help address it" – and then you talk to them about the most basic level of steps they should be taking and could be taking to protect themselves, and they're not even doing that. There have been some shifts in Canada in the regulatory regime and that will help speed things up a bit.

### Robert Parisi

We've seen a steady migration to viewing the issue as resilience as opposed to just security, but with security being part of resilience. With large organisations you've moved from having chief technology officers who would say, "we've bought computers and we have a lock on the computer room door", to chief information security officers, who think about "how are we going to manage this risk across that spectrum of our operations?"

So we've seen a real change but I've got a skewed view in that I tend to talk more to larger clients than to smaller clients, the latter often being more reliant upon third-party service providers for elements of their technology and security.

### Mike Senechal

We deal a lot with the smaller end of the market and there's a perception problem of what cyber exposure can actually be for small and medium-sized businesses. A lot of the smaller businesses say, "I don't carry people's credit card data so I'm not at risk".

We've certainly seen some instances in industries that you wouldn't think of. We know of a trucking customer out west. Someone got into their accounting packages and basically seized it. They didn't know where their trucks were, they didn't know where they were supposed to go. Those stories are starting to get out more and people are starting to understand the breadth of the risk.

### Dmitri Kralik

At Ridge Canada, we also deal with a lot of SME business. I was talking to a temporary staffing agency recently, it's a business that relies heavily on confidential data – for example, they're collecting SIN numbers [social insurance numbers] of all the temporary employees. It's a smaller business and their understanding of exposure was not there in a sense. The agency did not seem to acknowledge that even though a lot of their information was stored with an outsourced software provider, the responsibility to protect the information was ultimately assumed by them.

So size of business is definitely a big variable with respect to understanding exposure. With a lot of smaller clients, I would say they are still in the process of being educated.

### Phillip Hoyt

My focus also has been in the SME space, which is typically $200mn or less in revenue size. Within that group, we would see data-rich clients such as professionals, law firms, medical providers, who have an understanding of the privacy issues, but they lose sight of the financial risk exposure that they have.

One particular client I was working with had a product for heavy industrial/construction/mining/utility work. A lot of it was autonomous vehicles or autonomous monitoring.

"There's a perception problem of what cyber exposure can actually be for small and medium-sized businesses"

**Mike Senechal**

And they said, "I'm not really sure we need a cyber product". They didn't make the connection that a hack of those autonomous vehicles, that remotely monitor or manage the equipment, was a clear and present danger to them and their clients.

And then I've worked on programmes where through an affinity business, the real opportunity was just to hold your nose and provide a really low limit with half cover to a group, a large affinity of several thousand members – and then through that, and a marketing campaign and educational campaign with the broker, to then educate and up-sell real coverage.

So from that perspective, in the SME space, unless you are a data-rich, privacy-rich enterprise, it's not on the radar. If your broker tells you to buy it and the price is right, they will do that. Short of that, no.

### Tom Allen

That's an interesting point: an affinity group as a case study. You could look at 1,500 businesses who all do the same sort of thing. And since you work with an affinity group, you've got a pretty good idea of what they're dependent upon.

So they have vendors in common? What does it look like when the network is unavailable? Where are the pain points? Then you can emphasise an offering for them that

"A big difference between what you see in the EU with the [data protection] legislation, and in Canada and the US, is the class action risk"

**Ruth Promislow**

says, "here are five loss scenarios and this is how the product is going to react".

### Phillip Hoyt

In that sort of risk pool, offering a limit, even though low, was an affirmative ground coverage which then provided the defence on the non-affirmative other policies. And we stumbled upon the PEO [professional employer organisation] business in the States, which wound up being an amazing petri dish for SME cyber business because it's a vastly diverse group of industry segments in the PEO business.

And at the same time we could offer cyber to all these folks and then get a great cross-section of business. And then affirmatively carve coverage back, say, for a privacy or data-rich risk, even though it was SME. Which is an interesting way to cut your teeth and study your risk.

### Christopher Munro

Has the launch of GDPR in Europe helped fuel the growth of the cyber market as well?

### Tom Allen

For years in the London market, we talked about how GDPR will be coming along in a couple of years and everyone in Europe will have to buy cyber insurance. And it hasn't really happened yet. The responsibilities imposed by GDPR are more onerous than any equivalent legislation, certainly in the United States. The risk has arrived and it's sitting on insurers' doorsteps and I don't think we paid quite as much attention to how much rate this requires and what the claims experience is really going to look like.

### Ruth Promislow

A big difference between what you see in the EU with the legislation, and in Canada and the US, is the class action risk. In Canada there's been a lot of movement in the courts to open the doors to the privacy class action exposure for the organisations and the insurers. And the shift in the regulatory regime will fuel that fire of the class action risk. So that's where you're going to see, in part, the regulatory regime creating a bigger demand for insurance.

### Robert Parisi

Cyber insurance was originally built to cover the new risks of the dot-com economy. And then that bubble burst. And then we were starting to rebound and you had the first big D&O hit in 2000 and the 9/11 tragedy, and all the oxygen got sucked out of the room.

Then it kind of lay dormant for a while until California came along and you had the privacy breach notice statutes, which was like flipping the nitrous oxide switch. That's when cyber insurance took off, not because anyone necessarily had a better sense of what their risk was but they knew they now had an obligation that was going cost money to comply with, no matter what they did.

With GDPR, you can almost analogise it to Y2K which the insurance community got very excited about. Will it be real loss or won't it? Amongst large multinationals, GDPR is driving their compliance discussions but it's not driving their insurance discussions. And in part that's because they're looking at what's gone on in the US, and what they haven't seen is class actions that have resulted in large damage verdicts.

So while we thought in the early days that cyber would evolve like employment practices, we'd have some of the class actions, they would be interesting and then we'd get big verdicts, we never got the big verdicts – at least not the damage verdicts. And that took a little bit of the wind out of the sails. Fortunately, at the same time people started to recognise that cyber was really a property & casualty risk and we've been ignoring the property side of it. And that's what's now driving the growth of cyber. They're not looking so much at the casualty piece as they are at the property side of it – the lost revenue and damage to digital assets.

### Dmitri Kralik

You're seeing the requirement for cyber appear more in contracts. There's one example in the US with a major airline turning around and suing the chatbot provider that caused the breach that they had for failure to implement basic cybersecurity controls. If you start to see more sensitivity around relationships between companies and their suppliers and business partners, where a big customer can dictate the terms of the contract and they're able to point responsibility back to you – that will be another catalyst to growth.

### Robert Parisi

Historically there was a lot of confusion between professional liability and cyber, especially on the casualty side. People trying to sell professional liability to companies

that didn't need it and people confusing wanting to have a broad professional liability policy without cyber exclusions versus just putting cyber liability within the insurance requirements of a contract.

Again, I tend to bang this drum a lot – cyber insurance is really a property-and-casualty-based risk. Professional liability doesn't need to evolve, it's there; you just need to make sure you don't have the exclusions. But where we're seeing the change in the insurance community is on the property and the casualty side – the property probably more than the casualty. We are seeing the insurance industry wake up to that now with the move to address silent cyber.

### Christopher Munro

There have obviously been some big headline losses, but cyber underwriters are saying that rates are still soft for the risk. How do you view pricing in the market?

### Mike Senechal

It's a good one. Full disclosure: I'm neither a lawyer nor really an insurance person, I come from the tech side, but I've been involved now for a couple of years. I've looked at this one closely and certainly competition is a big component of this. You are getting a lot of new entrants coming in and there's a very large risk that you're going to start to create a race to the bottom, at the bottom end of the market.

The small and medium businesses are going to be the ones that suffer the most from what's happening on the pricing side. Because, again, it's the point made earlier by Ruth that businesses don't really understand what they're buying. When you combine that with the price sensitivity that's going on and the price pressures, you end up with these watered-down products that just don't serve anybody. It doesn't serve the end client, it doesn't serve the insurance market, it doesn't serve the broker. Nobody wins in this round.

### Angela Feudo

There's an excess of capacity for cyber. Everybody wants to be in it. Outside of the US, there's not a tonne of penetration, especially here in Canada. There's been a lot of M&A as well, so it's tough for organic growth. There's also more entrants, and the broadening of coverage as well. As the coverage broadens, if you're still providing the same rate or the same premium, that rate is actually getting smaller and smaller over time because you're providing additional limit or additional coverage. It's a tough market because the market hasn't fully realised the losses on the coverage that we've been providing for the last five years. And insurers are now providing additional coverage, but we don't know really what those losses are going to be. Unlike more traditional classes of business, we don't have the hundreds of years of data to look back at, to price the risk going forward.

### Ruth Promislow

I have an outsider perspective because I'm not in the insurance industry, but my impression, when I speak to people in the insurance market in terms of the underwriting, is I'm amazed at how few questions are asked or what the requirements are. And people say well, if we ask too many questions, they'll just go somewhere else. So I understand there's not the historical data that you typically have in insurance to inform pricing, so that's obviously one aspect of it. But at the same time, when I look at other areas of insurance where I've been involved, you can see a much more rigorous underwriting process. That has to feed into this soft market and has to have something to do with it.

### Angela Feudo

It depends on the size of the business in terms of the underwriting questions that are asked. For larger businesses, the exposure can be very complex and so there is a lot more underwriting that goes into them. For this type of business, we do have people come back and say we ask a lot of questions. But it's all about asking the right questions to make sure what we are providing meets the customer's needs and fairly prices the risk. Ultimately, the more information we can get about their risk, the better service we can provide.

### Robert Parisi

For large risks the underwriting hasn't changed really at all since we started that first product at AIG. It's a pen-and-paper governance exercise – with maybe a follow-up call with the CISO, that's largely what the carriers rely upon. What's interesting to me is watching the small and medium space; you have carriers who will underwrite with essentially no security questions. Tell me what industry

"Sensitivity around relationships between companies and their suppliers and business partners will be another catalyst to growth"

**Dmitri Kralik**

"As more markets start to recognise what cyber really is and where the real exposure lies, they'll start doing things like using property ILFs"

**Robert Parisi**

you're in, tell me what size you are, and as long as you're not in one of the industries I don't do, send me your cheque and I'll send you your policy. You have others who are very focused on particular industries, whether that's financial institutions or healthcare.

So it's a little bit confusing at times. You've had a lot of companies come into the space, dip their toe in the large risk, get on a $200mn tower, put a $10mn slug down and the next thing they know, they've lost $10mn.

So how do you pick and choose your battles? Because across the board the market has been relatively flat. The SME market has been incredibly aggressive and I've seen four or five markets over the course of the last two years exit the large space to focus on the SME space. And they're going into a rugby scrum.

The interesting piece is the companies now that are claiming to be able to underwrite using some kind of adaptive technology or AI, and somehow claim they're able to then better underwrite and can better pick and choose risks. And it's hard to say whether or not they've been successful. They may have been successful for the last two years but it could explode next year. So yes, it's hard to get clients to share information when they don't have to, it's hard to convince brokers to get clients to answer more information when there's not a commensurate price decrease or coverage expansion directly associated with the answer.

### Phillip Hoyt

The one thing that has really changed from anything I've seen in my entire career is how quickly a relatively new insurance concept moved from non-admitted. In the past we had a group of players in the non-admitted market who would stick to a certain script, and products tended to have a certain lifecycle before they went to the admitted market.

That period of time gave the entire industry the ability to look back and see what had happened and the ability to change terms and rates very quickly, and people could leave the market very quickly.

I'm still shocked at how quickly we had to compete in the non-admitted space with admitted cyber coverage. It really pushed prices down. So it keeps people in the game because they have to compete, and prices being pushed down because admitted carriers file rates in the US, and the US is the centre of the universe when it comes to cyber coverage. It keeps rates more stable and if they're low to begin with, admitted carriers are loath to go to regulators and make wholesale changes to their filings. So it's really held the non-admitted market down, which has suppressed pricing.

Cyber has become a property casualty product and an example would be how quickly we added bricking endorsements to cyber policies. My concern is that we're providing real property, bricks and mortar coverage on a bricking endorsement, and those rates look nothing like a property risk. We aren't even considering underlying individual risk characteristics as you would with a property risk.

### Robert Parisi

And I've heard a very jaded reason as to why the market has done this. It's because this is one of the only organically growing lines of insurance. The world isn't producing new public companies the way it used to – M&A goes up and down. You had some markets that got in aggressively and then pulled themselves out. But as more markets start to recognise what cyber really is and where the real exposure lies, they'll start doing things like using property ILFs [increased limits factors] as opposed to professional-liability ILFs and pricing the excess limits.

We've taken the time over the last 10 years to be that voice in the wilderness and tell our clients that this is a significant property risk. And they say "well, I buy $2bn of property. If you tell me that my largest exposure is not from fire or explosion in terms of business interruption, it's technology, unplanned tech outages or cyber breaches, then I'd better buy $2bn of that". And that's fine, but how do you do that if the market doesn't rate it the right way, if the market's not there and sustainable.

So we're at a bit of an inflection point as the markets start to understand this better and hopefully evolve in a way that allows them to be more sustainable. Because sustainability of the cyber market is as much a concern for me as a broker, because my clients are not going to want less cyber going forward, they're going to want more, and I have no real interest in a race to the bottom in pricing because that's a very short-term gain for everyone.

### Tom Allen

I agree that real rates have gone down as coverage has expanded because we've been adding to the contracts to

keep the premium stable in the primary market, and the excess market is a very competitive space. So it's kept prices flat as we've expanded and taken on a lot more risk. As a market we're therefore exposed to a lot of accumulation. And I would say most of the market doesn't have a very sound idea about the size of the wagers that we've made against our balance sheets.

From another perspective, claims are ultimately the product. Are customers buying the equivalent of the fire brigade, are they buying the response package, or are they buying a product to fill a gap in their existing cover? It's going to be different products for different buyers. But for them to get a price efficiency out of it, the process needs to look a little bit different for either different industries or different size of firm, or both.

When we look at business interruption exposures, for instance, the gross profit figure could be really overstating their real PML [probable maximum loss]. So there are circumstances where a more granular approach might save money and might yield also a better programme structure. But we just haven't really done enough to shift that paradigm of making these different approaches to the product available.

### Robert Parisi

We're at a point where we have got a P&C product that, with few exceptions, was developed and underwritten by financial lines underwriters. Now we are seeing the underwriters come in that don't have that legacy baggage of professional liability and can look at the product differently. We're starting to think about the wording, we're starting to think about the pricing, we're starting to think about the ILF, we're starting to think about what a business interruption worksheet looks like for cyber.

### Phillip Hoyt

You wonder how many cyber underwriters today have ever even seen a BII worksheet or knows how to calculate business interruption?

### Robert Parisi

There is a fundamental disconnect there. You have seen underwriters and brokers who are taking the time to understand that, and are building out expertise, and it's been matched in clients. We've talked about clients not understanding but you are seeing the board taking an interest in this and taking the time to understand what the company is doing. Now is that the same as doing some kind of penetrative or invasive testing, or sending engineers out? No. But at least it's a step in the right direction.

### Phillip Hoyt

It has to come from some direction because the limits are going to go up, the claims are definitely going up. We probably have just started to see the real impact of the bricking endorsement.

### Robert Parisi

Well the market dodged a bullet. If WannaCry and Petya had hit a server in Western Europe or North America, we wouldn't be talking $3bn-$10bn of loss. We'd be talking $10bn-$15bn – or even $25bn – and probably more companies that actually had standalone cyber insurance. But that wake-up call means more people now want the coverage so we as a market have to figure out how to provide it and provide in a sustainable way. Whoever can figure that out will make lots of money.

We've now also had at least two companies and the Lloyd's market say you must either exclude or include cyber risk for traditional lines of insurance and be unequivocal about it.

The general understanding, and certainly I'm happy if anyone thinks I'm wrong, is that the traditional markets are going to exclude it, not include. The casualty markets have already excluded it, and the property markets are likely to follow suit.

So you're going to see more of a demand for the bricking type risks, the semi-physical losses, come in and the cyber market has proven itself to be both acquisitive and adaptive and flexible and hungry. And most carriers will say, "oh we'll give that to you but not in your property or CGL policy, you've got to put it over there because those are our cyber underwriters, they know technology".

### Christopher Munro

With the move towards affirmative/non-affirmative cover, do you think the market on the SME side has got a true handle on the silent cyber issue?

"I'm still shocked at how quickly we had to compete in the non-admitted space with admitted cyber coverage"

**Phillip Hoyt**

"There's a lot of work going into being affirmative – saying yes, it's excluded, or yes, it's covered in other product lines"

**Angela Feudo**

### Dmitri Kralik

I know some larger carriers in Canada have started putting either affirmative or exclusionary language on all their policies across different coverages. At Ridge, we only focus on cyber insurance so the issue of affirmative/non-affirmative cyber cover isn't as applicable to us.

You're starting to see the wave turn in terms of increasing awareness about the exposure among SMEs and some realisation that you need a standalone cyber policy to ensure you are covered and not just rely on extensions on other types of policies. Clients are not just realising this after they've had a breach but more pre-emptive stuff as well. There are factors contributing to this education. The Canadian government, for instance, just released a cyber essentials programme, which is essentially an auditable cyber security programme and it's geared towards SMEs.

In terms of the rates and the competition, obviously rates are super sharp down at the SME level and I think that one of the other big components of competition is that as a greenfield space, there are still a large amount of businesses out there that are not buyers yet. You're not just competing against other syndicates and markets, you're competing against business' propensity to spend.

### Christopher Munro

Mike, what's your take on that?

### Mike Senechal

I agree with that. The exclusions are going to be good and I think it needs to happen. There's been a little bit of hiding from getting cyber because of that. So I see it entirely as a good thing that keeps the dialogue going, especially at the SME level. I would agree though that there's still inherent risk where SMEs just don't understand what they're doing and in a lot of cases it's compounded because they're outsourcing their IT to other IT providers. The worst-prepared industry for this is tech providers, particularly at the lower end, because there's just too much belief in themselves. That if someone hacks you, they'll just run their backups, and they just don't have the full understanding that, no, it's more invasive than that.

### Angela Feudo

There's a lot of work going into either being affirmative in one way or the other, saying yes, it's excluded or yes, it's covered in some of these other product lines. There's a lot of work also going into looking at the aggregation as well. Are we insuring what we intended to insure? And are we buying the right reinsurance as well to align with our corporate goals?

Because to Bob's point, we all need to make sure that this is sustainable going into the future because we're all going to benefit from that. The insureds will benefit, brokers will benefit, insurers and reinsurers, to make sure that cyber cover is around forever.

### Christopher Munro

Fantastic – thank you very much for your time everyone.

# Inside P&C

## Dedicated to the US P&C market

**Inside P&C is a new service covering American insurance markets.** A US product with a US voice, for a US audience.

Brought to you by the same publishing house that produces ***The Insurance Insider***, ***Inside P&C*** will provide unparalleled market intelligence on the entire US P&C market – from small commercial and personal lines right through to reinsurance and Bermuda.

## What will the readers receive?

- **Daily** Competitive Intelligence briefings – curated by the Editor and delivered straight to your inbox
- **Punchy and pithy insights,** reviewed by expert analysts and built to act upon
- **Real time** market intelligence drawn from a wide network of industry sources
- **Full access** to insightful, in-depth reports
- **Invaluable** business intelligence that adds context and perspective. Responsibly sourced by an award-winning Editorial team
- **Fast-response analysis** of important news that helps connect the dots
- **High-value** commentary on key companies and industry themes

**NOW LIVE**

**insidepandc.com**

THE INSURANCE Insider


## Let’s turn digital threats into client’s trust.

Find out more at munichre.com/cyber

NOT IF, BUT HOW

Munich RE