Autumn 2018

THE INSURANCE Insider

CYBER ROUNDTABLE 2018

Big data or Big Brother?

Scanning technology could hold the key to measuring cyber risk, but clients may take some persuading…

Insight and Intelligence on the London and International (Re)insurance Markets
www.insuranceinsider.com

In association with
Barbican INSURANCE GROUP

BARBICAN CYBER OSA

ONE STEP AHEAD

In a changing world,
the wise stay
one step ahead

Barbican Cyber OSA – *value adds for our cyber insureds*

Barbican
INSURANCE GROUP

Barbican Cyber OSA currently offers three value adds to bolster critical aspects of your cyber security strategy: cyber threat reconnaissance; cyber phishing defence; and cyber intrusion response.

For every $15,000 in net premium with Barbican you can choose one value add; spend over $30,000 you can choose two value adds, spend over $45,000 and get all three.

	Indicative Market Value
CYBER RECONNAISSANCE **FICO Cyber Risk Score (CRS) Portrait** Identifying externally visible weak spots and red flag indicators that could attract system intruders. Providing clear actionable insights on how to improve your cyber posture.	$10,000-$50,000
CYBER PHISHING DEFENCE **TSC Advantage Phishing Simulation** Controlled phishing and spear-phishing attacks to see how many employees click on the cyber bait. Providing recommendations on improving attack resilience.	$10,000-$15,000
CYBER INTRUSION RESPONSE **TCS Advantage Incident Response Exercises** Combining table-top incident response exercises and in depth documentation review. Providing a detailed evaluation report on how to improve your cyber intrusion response.	$10,000-$15,000

www.barbicaninsurance.com

Connect with us

Big data versus hackernomics

What makes a good cyber underwriter?

It's a question that all underwriters in all lines of business ask themselves, but for cyber it feels a little more difficult to answer.

Unlike hurricane risk, which has changed little in centuries, cyber risk changes daily. It can evolve in previously unimaginable ways, varies vastly from insured to insured, and has the potential to be enormously systemic.

There's a huge onus on cyber underwriters to remain on top of the risk, recognise their insureds' vulnerabilities and, of course, price risks accurately.

The Insurance Insider's third annual cyber rankings survey found that brokers value knowledge and experience the most in underwriters.

So should the cyber market be using as much data and technology as is possibly available in order to build that knowledge and understanding?

At this cyber insurance roundtable, participants discussed that very topic.

Around the table were underwriters and brokers, as well as experts from FICO, a firm which made its name in providing credit rating scores but has now extended that methodology to cyber security.

At the crux of the debate was whether scanning and scoring technologies were more successful in assessing how vulnerable a client is to a cyber attack, versus a more macro view of the threat landscape – often known as "hackernomics".

This led to more existential questions around the extent to which underwriters should rely on this information to price risk.

Can the data available ever really keep up with the ever-changing nature of cyber risk? Do scanning technologies really work when many cyber losses stem from human error? Does human gut instinct still have a part to play here?

Brokers around the table argued that while underwriters certainly benefit from having more data available to them, giving a client a score on their cyber security could actually make cyber insurance a harder sell, particularly if a bad score triggers a negative reaction.

Equally, how do clients really feel about their insurer taking a "Big Brother"-type approach in assessing their risk?

The questions being tackled by the cyber market today will undoubtedly become more pertinent to the rest of the market in the years to come.

Underwriters in the property cat or marine markets may argue they have a good grasp on the risks they need to price. But in a market where margins are fine and capacity is plentiful, the effective and smart use of technology will offer a real competitive edge.

Soon there will be an arms race in building these capabilities, if it hasn't started already.

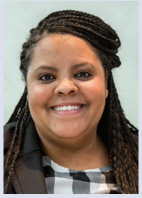
A rousing – and sometimes heated – debate was had at our roundtable as participants tackled head on the big questions around the use of big data and technology in underwriting.

It certainly made for an interesting session and I hope the debate continues in the years to come.

Catrin Shi
News Editor
The Insurance Insider

Roundtable participants

David Dickson
Head of Technology and Cyber, SafeOnline



Shannan Fort
Cyber Product Development Leader, Aon

Manish Karir
Director – Cyber Insurance Solutions, FICO

Geoff Keig
Regional Director, Stackhouse Poland Ltd

Graeme King
Business Group Leader – Cyber, Barbican

Kimberly Manibusan
Director – Cyber Insurance Solutions, FICO

Darren Vye
Senior Claims Adjuster – Cyber, Barbican

MANAGING DIRECTOR: Mark Geoghegan
mark@insuranceinsider.com

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

MANAGING EDITOR: Charlie Thomas
charlie@insuranceinsider.com

EDITOR: Laura Board
laura.board@insuranceinsider.com

NEWS EDITOR: Catrin Shi
catrin.shi@insuranceinsider.com

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

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

SALES DIRECTOR: Rob Hughes
rob@insuranceinsider.com

BUSINESS DEVELOPMENT MANAGER:
Benjamin Bracken *ben@insuranceinsider.com*

SALES EXECUTIVE: Annie Lightholder
annie@insuranceinsider.com

MARKETING MANAGER: Aimee Fuller
aimee@insuranceinsider.com

HEAD OF EVENTS AND MARKETING:
Jennifer Lord *jennifer@insuranceinsider.com*

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

EVENTS PRODUCER: Sally Kramers
sally.kramers@insuranceinsider.com

EVENTS AND MARKETING EXECUTIVE:
Holly Dudden
holly.dudden@insuranceinsider.com

PRODUCTION EDITOR: Ewan Harwood
ewan@insuranceinsider.com

SENIOR SUB-EDITOR: Tim Peters
tim.peters@insuranceinsider.com

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

Published by: Euromoney Trading Limited, 3rd Floor, 41 Eastcheap, London EC3M 1DT, 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. 2018 Euromoney Trading Limited,. All rights reserved.

Cyber
Roundtable 2018

Catrin Shi
Graeme – do you want to kick this off and talk about why we're all here today?

Graeme King
For a long time there has been a need for more reliable underwriting of cyber risk, and that means using technology where possible to understand more about the risks that we're writing. For example, you'll get an application form which ticks certain boxes and suggests that the client has certain good or bad features. A price is then calculated from that, often based on a relatively limited amount of historical cyber data. How do we know that what we're being told in the application is an accurate reflection of the client's cyber risk? And is there data out there in the world that could help us answer that question better?

There is a growing number of technologies that have evolved and this is a good time to test how strong the case is for using available data and applying it in the right way, to help underwrite the risk better.

> "For a long time there has been a need for more reliable underwriting of cyber risk"
>
> **Graeme King**

Catrin Shi
We also have two representatives from FICO here today. Can you say a little about what FICO does?

Kimberly Manibusan
FICO offers analytic and decision management tools in a number of industries, including banking and insurance. We currently offer a cyber risk score for not only the cyber insurance underwriting market but also focusing on the enterprise world in assisting them to understand their external cyber security posture. Our solution is leveraged by underwriters and brokers, but also focuses on the chief security officers, IT managers and risk officers within the enterprises.

Manish Karir
The reason FICO is in this space is because we have built a score that's very similar to the FICO consumer credit risk score. The ideas are similar – it's a way to collapse large volumes of data into a single, or very low, number which then becomes actionable.

One of the problems with very large volumes of data is that they are diverse – they can tell you two different things, depending on which subset you look at. But if you collapse it down to a single number then that can become actionable. It's a number you can make decisions from and that's FICO's goal in this space.

By generating the FICO consumer score, we enabled massive amounts of credit to become available to individuals. We envision bringing that same capability to the cyber security marketplace and in particular cyber insurance and risk estimates.

Catrin Shi
To what extent can the cyber insurance market use artificial intelligence (AI) and big data to assess cyber risk, and how much are companies doing this at the moment?

Manish Karir
What helped us build what we have today is that six, seven, eight years ago, we were looking at large amounts of global data and, in particular, malicious activities. With the patterns that were embedded in those large data sets, whether it's phishing or spamming or other kinds of fraud that are taking place on the internet, we started to notice that there were natural clusters around those events.

That got us thinking – why do these clusters exist? There must be some properties about these particular neighbourhoods on the internet which make them more or less susceptible, and they must be properties that we can measure, so what properties can we measure at scale globally?

We started to build upon that with large data collection capabilities that were available to us, and we started to understand that the difference between the good and the bad neighbourhoods was that policies and policy implementation on the ground were different.

If we can see policy variations on a country-by-country basis, then the next step is to see policy variations on an organisation-by-organisation basis – so we started to investigate those. You can look at individual companies on the internet and by understanding their footprint, look for the cyber security signals they are generating and, from those, understand whether or not those signals are going to lead to a greater or lesser risk of data breaches.

Graeme King

Most of us in the room are familiar now with that type of technology – big data and the scanning of companies. What are your feelings about scanning technology generally – is it good or bad, does it work, does it have limitations?

David Dickson

It's great for opening a client's eyes to the fact that potentially they're not very mature around their risk and the insurability of the risk, but there are certain limitations. While malicious third parties or system glitches account for many claims, there's always subjective human nature which needs to be accounted for and there will always be an asterisk next to every result. It's very important, and that harvesting of data will inform distribution and also the products and the claims, but it's not the entire picture.

Shannan Fort

If we are talking about external scanning, where essentially the client has no knowledge of it taking place, I would have to disagree. Generally, when those reports are presented to a client, it tends to put them in a defensive posture. They're starting with a company that already has a perception of the business, without any mitigating elements, and they are having to defend what they do and why they do it, as opposed to describing and explaining their business to them. That puts everyone in a more negative position.

The other thing is that I have been in the position more than once where you're having to defend a client to an underwriter because of a report they've received from a third party which has done some sort of external scanning, and the client has received a very negative score.

There may be mitigating controls – it may be what they are scanning is no longer relevant. So instead of starting at step one, we're now starting at step negative five, and already you are thinking about increased rates and restricted cover.

Manish Karir

That's a valid concern and there could be inaccuracies that automatically create this bad relationship with the client. One of the important things to remember is the voice of people who are approaching organisations to purchase insurance. We are careful about making sure that they have a say in how they're scanned or profiled, whether they want to opt out of the process, or whether they want to come in and say, "I want to help you get this right, so you don't create the wrong impression when you are getting a policy for me". The subjects being profiled must have a say in the process.

> "Not every scoring/external scanning technology is created equal. It's important for the insurance community to understand the detail behind how these scores are generated"
>
> **Kimberly Manibusan**

Kimberly Manibusan

The other thing that is important to note is that not every scoring/external scanning technology is created equal. It's important for the insurance community to understand the detail behind how these scores are generated, the model development and data that is collected. Transparency around these areas is critical to the underwriters relying on such metrics.

Graeme King

As a concept, the use of big data seems very appealing. But is it something you feel that, used in the right way, could ultimately benefit you, as well as the client, when you're trying to broker risks and assess them?

David Dickson

The good thing for you is that it does take an objective view on like-for-like companies, so you can look at a portfolio of manufacturers or accountants, or a similar sort of risk, and say that this is the common issue or shortfall that we're seeing. If that information is then shared with brokers, we can help inform clients about things they should be looking at.

Shannan Fort

On the one hand, we absolutely need big data – we need this idea of grouping together large data sets to draw some conclusions about risk, to make the underwriting process

"Cyber is still quite new, so it's hard to establish any real claims trends. We've seen lots of notifications, but very few major claims"

Darren Vye

more efficient and to build predictive better models around losses.

On the opposite side, each risk is a unique risk from an underwriting perspective. No two companies, no matter how similar, are going to have the same security setup. There will be different mitigating controls and processes and you can only learn about that from actually underwriting the risk.

Clients are looking for more certainty about the types of losses that they're actually going to suffer, and to better understand what cyber risk actually means for them and their peers. So when we get to a point where that big data meets unique risk, benchmarking information then becomes usable and real and something that we can all utilise on the front end. But we're not there yet. Technology is changing very quickly and we are constantly having to innovate to address new dynamics.

Geoff Keig

First of all, it depends on the size of the risk you're trying to broker. With large companies, you're going to broker them individually and you're going to have a lot of data sets relevant to them. But there's a sector relevance too that insurers are going to use and big data is going to help analyse that.

There are limitations with all of these things and, of course, all risk, particularly cyber, is going to be two-pronged anyway – it's people and processes. You can't solve one without the other. But if you can stop half the risks getting to your people by using technology, then you're only training on half the access and that has a real benefit in terms of the losses people suffer.

So are the clients saying this risk score is wrong? Because if it's right, it's still relevant, even if they don't want to hear it.

Graeme King

The issue is the readiness of the market to accept this type of technology and how it's used to generate probabilistic scores. The credit scoring market isn't a bad analogy here. I'm guessing that in the early days of that, there was probably a similar scepticism from many people.

Kimberly Manibusan

There were a lot of challenges for FICO early on in the consumer credit space in terms of initial market adoption and understanding of the score output, but now the FICO consumer credit score is utilised in almost 95 percent of consumer lending underwriting decisions in the US.

Geoff Keig

Shannan is right. The problem is that the rate of movement in the cyber sphere at the moment is exponential. It's still useful, don't get me wrong – all of the technologies have a role to play – but this is not a one-solution answer.

Catrin Shi

Part of the problem here is that there isn't much data out there at the moment – not in the sense of how property cat has been modelled, for example. Cyber is nowhere near that and the risk keeps evolving. Darren, do you have any insight from the claims side on this?

Darren Vye

Cyber is still quite new, so it's hard to establish any real claims trends. We've seen lots of notifications, which either haven't materialised or exceeded the retention, but very few major claims. This gives us limited data to predict the likely outcome of different events. It's just going to take time. Once we start to see more frequent claims we will be far better placed to analyse trends.

Catrin Shi

On the other side of the spectrum from the rating technology is assessing the threat landscape – hackernomics, that sort of thing. Could you use these in tandem to give a "best of both worlds" scenario?

Graeme King

It's one of the biggest questions I ask myself. I'm a user of this type of scanning technology and I understand it has its limitations. But when it comes to the threat landscape, there are some very powerful arguments for understanding the external threats to your organisation, such as from the dark web, for example. It's not really good enough just to look internally. I would love an empirical answer to the question of how relevant it is to measure the threat landscape or whether it is sufficient to satisfy yourself that a company has locked itself down and has all the right procedures in place.

David Dickson

When you're looking at that and assessing a company from the outside, you're looking at a company at one moment in time. There are so many reactive issues and all sorts of triggers for external threats, so while you can get an idea of the space they're playing in through the traditional underwriting method, there's always going to be that unknown. I'm not sure what will counter that.

Shannan Fort

You certainly can't have one without the other. If you're only managing or owning one aspect, you're missing completely several aspects. We all know that nothing can be locked down completely, so you absolutely have to understand the threat landscape to understand what you're trying to lock out.

Taking it back to the conversation about FICO scores and how they're comparable to "cyber scores", I can certainly draw the data line, but at the same time I would argue that with the FICO score, you're judging a homogenous group. I still struggle to see how we can create the FICO scores of cyber and make it relevant in the next 10, 20, 50 years until technology stops moving as quickly as it is now.

Kimberly Manibusan

Remember we're looking at how the organisation is managing their day-to-day cyber hygiene from a policy and management perspective. It shows a lot about the organisation's operations on a day-to-day basis if they continually leave the firewall open for a period of a month and continually allow that to remain unaddressed and vulnerable. That suggests that there's an issue with the training and that the people who were supposed to be managing a web server, a laptop or network are not following cyber best practices.

Manish Karir

It's difficult to be resilient to changes in technology, which is why we try to look at what is behind the use of the technology. It's only when you get to that level that you end up with something that can be protected, because if you focus on technology failures, those are point-in-time failures and you will get those wrong, every single time. It's not about saying, "I see you didn't pay your bill here and here and here". If I look past that and say, "You're missing bill payments every other month", that's the pattern that's interesting and predictable.

Shannan Fort

That's what makes me incredibly nervous about this external scanning technology. It's the inference that is coming from monitoring points in time, even over a period. What if the firewall was down for a month because they were running some type of analysis or just examining their threat landscape externally? What if there's a risk? That's not something that can be inferred. How are we getting from the information that we're collecting to the inference? What is building that inference? That's where we really get tripped up.

Geoff Keig

The difficulty here is if that pattern of information is given to an underwriter who elects not to have a conversation based on the information they have, that's when it really starts affecting clients. If there is a new head of IT, or security officer, or a new COO – whatever the change is in the organisation that hasn't manifested itself but will do – how do you get to tell that story if you're already blocked from the market? This is where the real difficulties of some of the automated technology can come into play.

Manish Karir

The context is always very important. It's important to remember that the assessments are in general probabilistic, in that they represent a population. In a population, there is a given statement of risk that will hold true, but for any given individual, it may or may not hold true.

When you look at these large populations and you do these assessments in large groups, you start to see the statistics hold, and the probabilities of certain behaviours being correlated with data breaches hold as a population. Whether they will hold for that one particular client that you're trying to underwrite depends on particular circumstances. But if you had 100 of those similar patterns, identical clients, then you would see those behaviours hold true.

Shannan Fort

To Darren's point earlier, did you have enough data sets to make those inferences?

Manish Karir

Yes – we're looking at historical data breaches and that's how we're identifying the patterns we're picking up. FICO has

"It's difficult to be resilient to changes in technology, which is why we try to look at what is behind the use of the technology"

Manish Karir

been collecting data for the past four years, which is very small compared to property and casualty loss models, but 10 years from now, we'll have 14 years of data.

Shannan Fort

I wonder whether, in 14 more years, those patterns will have changed, and those inferences that you are able to draw will be wildly different to what they are now.

Graeme King

As an insurer which is currently in the early days of using this type of technology, we're being very cautious about how much weight we give to the scoring. We want to be able to compare the trends we see through our own traditional underwriting methods against the view the scanning technology gives us of the organisation. We are looking for our own correlation.

I say this when I'm trying to reassure the brokers that we're using this technology purely to help us better understand the risk. We can then have conversations with clients about the protection they have in place and be able to justify why a low score is not as bad for us as it may appear.

Catrin Shi

Talking more broadly about how clients view the use of these technologies as part of insurance products, do they demand it and does it help you with the sale?

"There is more board-level recognition around cyber risk and certainly around how a cyber event can impact individual directors and officers"

Shannan Fort

Geoff Keig

We operate in the small and medium-sized enterprise (SME) to mid-corporate market and many of our clients don't go to that sort of granularity. Also, they don't understand that actually they're already involved in dealing with AI every time they fill in a Captcha. They're not seeing the threat analysis that's out there, partly because they're not being spoken to on those terms, and that's probably the right thing because there is a staged process they need to go through in order to get there. Higher-end users will start doing their own threat analysis, but that's something that, for the type of client we're talking to, is relatively in its infancy.

If you look at where losses are coming from, it is from human interaction – it's not technology that's letting them down. So we're trying to educate our clients to change the way they look at their people.

Darren Vye

We need to make the client aware of that fact that risk-mitigation tools are there to assist them. We want to make our clients better at managing cyber risk. I totally understand why clients might feel defensive about a low score. This is where we need to highlight the positives and explain that the recommendations are there to help them reduce the likelihood of a cyber attack.

Graeme King

To some extent there's a good analogy in the use of black boxes for drivers. Those who are willing to take a black box are the ones who know that they're going to turn that corner in second gear, nice and slowly, who won't take a bend too fast or drive too late at night or break the speed limit. They recognise that it's a positive benefit to them because they're doing all the right things.

Corporates are far more complicated beasts than that individual driver, but it's a similar mentality to some degree. It's about how confident you are about your own cyber posture and how open you are to accepting something that's perhaps giving you a fuller picture of your cyber posture.

Geoff Keig

It goes back to a snapshot in time though, because if that snapshot is reflective of the last three years' data that you picked up about a business, and the business made an acquisition and saw 50 percent growth, that acquisition actually brought in behaviours that have changed over time. But formulating the risk picture up to this point is not the same as the risk picture going forward. The exposure to corporates is different, but they'll be doing a lot more analysis of their own risk than SMEs or mid-corporates will be.

Manish Karir

In insurance terms, what we really want to be careful about is avoiding moral hazard. Where you're not just providing insurance as a risk transfer mechanism, you want to make sure there is enough information available to all the right parties where there's a risk mitigation that takes place. Without risk mitigation, you will end up with only the bad risks, and so you have to be able to provide information to the end clients where they can understand how their behaviours matter and change them.

Catrin Shi
How do clients view these additional technologies being used in the underwriting process? Do they even know they're there?

David Dickson
We always portray the message that this makes up part of the underwriting, but not all. From our perspective, all they're doing is looking at something and it's a tick box, like most application forms. We are very cognisant of the fact that at the moment it can't make up the entire underwriting process – it's only one part.

Graeme King
At this stage of the evolution of this type of technology, it is absolutely the wrong thing for any insurer to rely solely on that score, or that scale. But it's where we may be headed with this in the future. I believe we will see a time when there will be far more standardisation and understanding of the factors which give a particular organisation a particular score. Once we reach that point, it will be a much simpler sell – in fact, the client would almost expect the insurer to have that information at their fingertips.

Catrin Shi
The wider casualty market has been dealing with that human element of exposure for many years and the predictive side of casualty modelling is not that well developed. Surely underwriters have been dealing with human error for ages?

Geoff Keig
What's really interesting is that we need humans to be enabled by the workplace. If we don't enable them then you're going to start losing productivity and all the other things that give you competitive advantage. At the moment the security protocols that insurers particularly like seeing in operation – lockdown and things like that – are sometimes in competition with and in conflict with enabling people. What I'm really encouraged by is the new kind of training that's come about, using psychologists and people like that.

Graeme King
You raise a very good point around just what it would take to educate the average person about the dos and don'ts when it comes to protecting yourself in a cyber environment. As an underwriter I live and breathe cyber risk all the time, so for me it's second nature now not to click on that dodgy looking link. The reality is there are so many people out there who haven't yet understood the importance and significance of the cyber threat.

Geoff Keig
Big data has the capability to monitor your social networking, look at your emails at work, link the two together and work out whether you're a disgruntled employee or not, and therefore are an increased risk to the organisation. Now that's a bit Big Brother for a lot of people but it's here and it's relevant and people need to start understanding that.

There are those businesses that say we have to empower people, let them do what they want to do and come to us with the problem because quick problem solving is important. We can't stop the problem; we just have to get the right behaviours in people to stop it as much as we can.

"There's been some enhancements in the distribution of cyber products and bringing the client much closer to capacity"

David Dickson

Shannan Fort
This raises an interesting thought. You have already mastered this idea of predictive behaviour for humans. Is that not something that can be translatable here – predictive behaviour for humans within an organisation and how that then impacts the organisation's cyber risk?

Maybe the focus is shifting away from how the system itself is protected, as opposed to the corporate culture and behaviour within an organisation – predicting how often it will be that someone will click on that dodgy link, and what type of training translates into better corporate citizens.

Manish Karir
I absolutely agree. If we could measure one thing at an organisation, we would measure people and culture. We can't do that at scale externally – we can't send surveys out to the entire global population. So we look for proxies that help us infer people and culture and the proxy measurements that we're making are the ones that we can do on a global scale. You look for whether or not the network admin team knows how to use patches on their systems regularly. We then send them a survey to ask them whether staff have taken a certain training model – we inferred that based on the data we collected.

Catrin Shi
I want to ask about what is driving the purchase of cyber insurance more generally from the clients' perspective.

"People might not have bought [the cover] because of GDPR, but GDPR was an excuse for brokers to talk to clients about cyber cover, so it did drive distribution"

Geoff Keig

David Dickson

Awareness, more of a media presence around these kind of breaches, GDPR [General Data Protection Regulation], and also more availability. There's been some enhancements in the distribution of cyber products and bringing the client much closer to capacity, both here and on the other side of the pond as well – whether it's from traditional brokers going a step further towards the client and offering retail products, or some of these bolt-on packages that they're getting as part of their home or buildings insurance. Perhaps as part of contents insurance as well.

Shannan Fort

I would generally agree with all of those points, but I would also say that there may be a million different factors at this point. There's more board-level recognition around the risk, and there's certainly more board-level recognition around how a cyber event can impact the board and impact the individual directors and officers.

What has certainly driven a lot more interest in the product over the past couple of years is the real-life impact that these issues will have. There are lots more contractual requirements these days for security and cyber cover.

To date GDPR hasn't been a massive driver, in the way that people may have anticipated when the regulations were first introduced. It might start to drive it a little more – especially once we start seeing some fines imposed, if those are insured, or even costs around the proceedings themselves.

There's also more and broader cover available. We've done a much better job over the last couple of years in expanding the cover so that it's relevant to more than just data aggregators.

Geoff Keig

People might not have bought [the cover] because of GDPR, but GDPR was an excuse for brokers to talk to clients about cyber cover, so it did drive distribution. The last statistic I read was that 50 percent of brokers are still not talking to their clients about it, but for those of us that are, it's both a wedge product and an opportunity.

There are compelling factors why people ought to understand this and the opportunity for us to talk to clients about it, through GDPR and other things, means that we've had much greater success over the last 12 to 18 months in converting potential buyers into buyers than we have done in the past.

David Dickson

The cherry on top as well is that this is the best time ever for clients to buy the risk coverage and it's cheap.

Kimberly Manibusan

FICO has just conducted its second annual "Views from the C-Suite" cyber security survey, and part of the survey covered enterprises' purchasing of cyber cover. We learnt that close to 70 percent of the healthcare organisations have not had cover, so there are areas that are still highly under-penetrated and don't have cyber cover.

Catrin Shi

Graeme, do you have any final thoughts?

Graeme King

This debate has been fascinating for a number of reasons. It highlights that there is a very different set of drivers behind our behaviours. The brokers have a specific need to place a product with a client, and that client naturally wants to give as little information as possible in order for that coverage to be given to them. If the coverage is readily available, for relatively limited information, why would anyone push the client to do more?

The underwriter, on the other hand, has the job of trying to assess risk, often with relatively limited information and often with information that's not as robust as it should be. Therefore, they're looking for ways to help them to underwrite those risks more consistently – and we've heard today the different needs of the different actors in this.

But we've also heard that there is a real need for a way of measuring the cyber risk of an organisation – whether it's external scanning of assets or scanning of employees. It's already being done. Sometimes it's accepted, sometimes not, but we're in the early days of the adoption of this type of scanning. In 10 to 15 years' time when we see this technology being routinely used and trusted, I believe it will put us all in a much better place.

Catrin Shi

Thank you for a really good discussion.

BARBICAN CYBER OSA

ONE
STEP
AHEAD

In a changing world,
the wise stay
one step ahead

Barbican Cyber OSA – *value adds for our cyber insureds*

Barbican
INSURANCE GROUP

Barbican Cyber OSA currently offers three value adds to bolster critical aspects of your cyber security strategy: cyber threat reconnaissance; cyber phishing defence; and cyber intrusion response.

For every $15,000 in net premium with Barbican you can choose one value add; spend over $30,000 you can choose two value adds, spend over $45,000 and get all three.

Indicative Market Value

CYBER RECONNAISSANCE

$10,000-$50,000

FICO Cyber Risk Score (CRS) Portrait

Identifying externally visible weak spots and red flag indicators that could attract system intruders. Providing clear actionable insights on how to improve your cyber posture.

CYBER PHISHING DEFENCE

$10,000-$15,000

TSC Advantage Phishing Simulation

Controlled phishing and spear-phishing attacks to see how many employees click on the cyber bait. Providing recommendations on improving attack resilience.

CYBER INTRUSION RESPONSE

$10,000-$15,000

TCS Advantage Incident Response Exercises

Combining table-top incident response exercises and in depth documentation review. Providing a detailed evaluation report on how to improve your cyber intrusion response.

www.barbicaninsurance.com

Connect with us