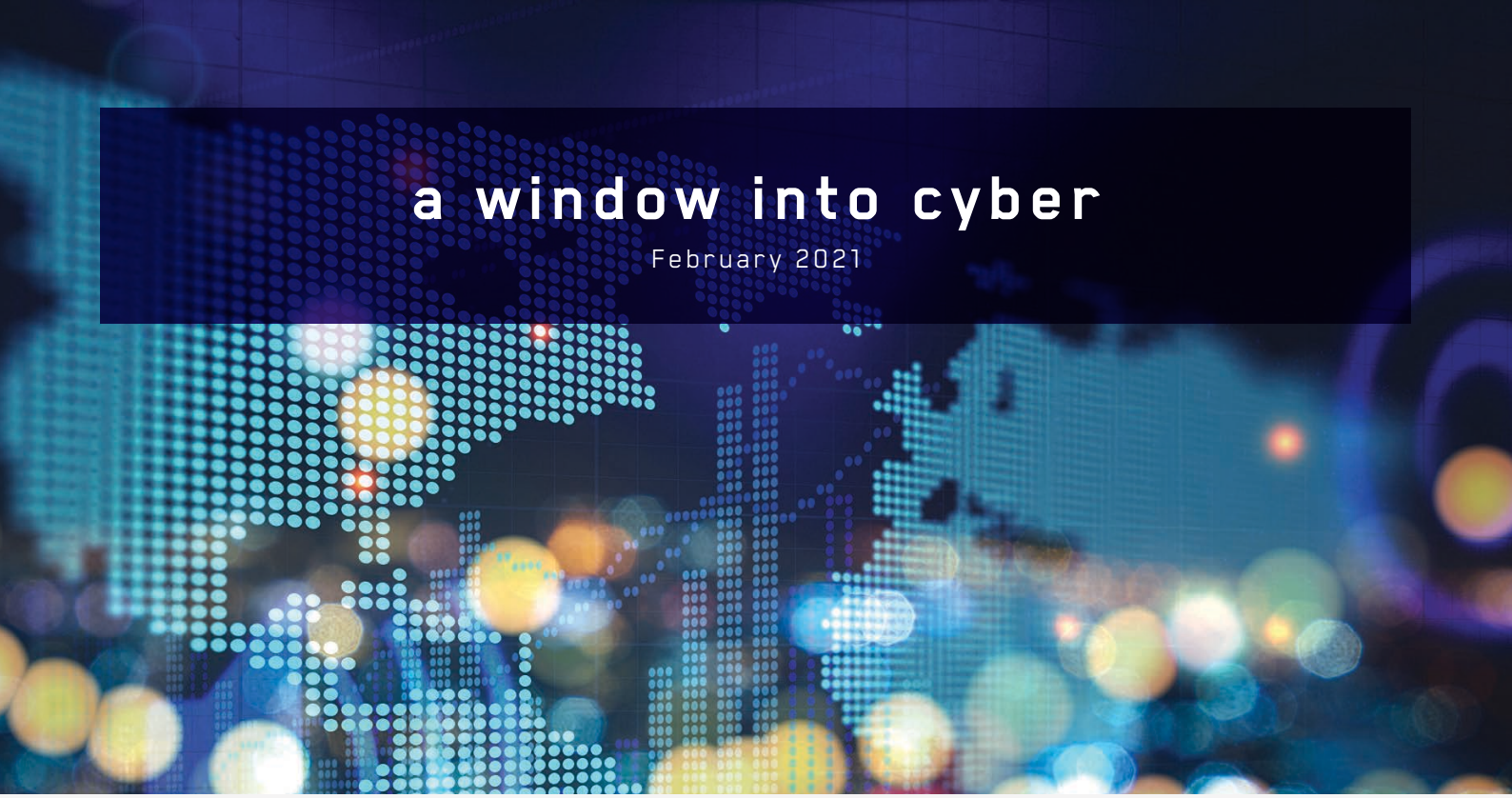

a window into cyber

February 2021

a note from Ben Maidment

Class Underwriter, Brit Cyber Services

BRIT

The increase in ransomware attacks in 2020 was both dramatic and profoundly alarming. From government agencies and large corporates to healthcare providers and SMEs, every type and size of organisation proved to be vulnerable.

An already bad year ended in the worst possible way. In December, news broke of the SolarWinds hack, which directly impacted over 18,000 US government and private customers. The after-effects of this colossal breach, many of which are as yet unknown, will likely last for years.

For insurers, the year ahead will be challenging; both in terms of pricing and the amount of underwriting due diligence required. Insureds will see premiums increase and may also see retentions rise and coverage restricted if they can't demonstrate the sort of ransomware mitigation procedures Insurers now expect. The cyber landscape has altered irrevocably but not everything has changed.

At Brit we've always taken a case-by case approach and that remains as true today as when we started writing cyber cover 16 years ago. What's more, our partnership with Datasafe continues to provide clients with the tools they need to proactively evaluate and manage their risk exposures.

Whatever 2021 holds, we'll be helping our clients stay on the front foot – so they can face the future with confidence.

BRIT

thoughts on 2020

As we started the year, we thought it would be a good time to take stock. So a few of our team got together (virtually, of course) to reflect on 2020 – and assess how the cyber landscape looks right now. Here are some extracts from our conversation.

on the call:

Ben Maidment – *Class Underwriter*

Adelle Gruber – *Senior Cyber Privacy Technology Underwriter*

Ed Hart – *Underwriter*

Connor Corcoran – *Underwriter*

Georgia Drew – *Assistant Underwriter*

BM: When the pandemic started and organisations began transitioning to remote working, I had genuine fears about what that could mean in terms of potential cyber losses. I think we were all concerned about what might happen; companies unable to cope, or not set up well enough for the changing work dynamic.

CC: But that doesn't seem to have happened. Most companies – and Brit's a good example – transitioned pretty effectively. And although it's led to new ways criminals can infiltrate networks, or get people to behave in ways that lead to something going wrong, things have carried on remarkably well. We have seen companies recognising more than ever the importance of good cyber security and investment in staff training.

> "We have seen companies recognising more than ever the importance of good cyber security and investment in staff training."
>
> *Connor Corcoran*

AG: I was pleasantly surprised at how well companies who were forced into their digital transformation managed – and actually accelerated – it. Think about the calls we were having a couple of years ago: there was very little indication that many of them were prepared for remote working on such a scale.

BM: But the rise in ransomware during the year was genuinely alarming; with attacks escalating in number and becoming more sophisticated. And the SolarWinds hack was the sting in 2020's tail; the implications of which could be felt long into the future.

But people are still making mistakes aren't they?

BM: Yes – and the main issue is probably still the human factor. The biggest weakness that a network can have is its people. Companies are getting much better at educating their staff about social engineering, email hygiene and so on. But it's astonishing how often that's still the reason networks are infiltrated. It's impossible to completely eliminate.

continued on next page

Are some industries better prepared than others?

CC: At first glance, you'd say that tech companies are more geared-up to defend themselves. But of course they have more data – and more reliance on digital processes, so there's certainly pros and cons there.

AG: Every sector has its own exposures. The focus used to be on the data-heavy industries with all the regulation around that and the need for breach notification. But with the rise of ransomware and its business interruption costs, that's all changed. We're seeing manufacturers – and other businesses that don't necessarily hold a lot of data – with significant tangible exposures.

Are most industries waking up to that?

BM: Ransomware's been a game-changer. Whereas risks such as business interruption for a manufacturing firm were apparent to risk managers, it's taken something like ransomware to put those types of risks onto the front pages; a bit like big data breaches did for data privacy a decade ago.

EH: The fact that it's now so frequent, with high-profile companies being impacted and making headlines, has changed perceptions and made businesses much more aware of their exposure.

Yet there's often more at stake for SMEs than for large organizations isn't there?

AG: Size doesn't matter! For an SME, losing a single contract or client could have a material impact on their ability to continue trading. That client may comprise a larger proportion of their income than a similar size contract for a larger company.

CC: And some smaller businesses rely on larger third parties, so when the supply chain is infiltrated, it's generally the bigger company that makes the news. A crucial difference is that larger businesses generally have their IT capabilities in-house, whereas many smaller businesses outsource this function to someone they trust – and that's where gaps in ownership or responsibility creep in.

GD: I'd say we're seeing probably more first-time buyers in the SME space – and they're often spurred-on by an incident or claim.

continued on next page

Are you constantly refining the wording to make sure that it's always fit for purpose?

BM: Yes we are. The pace of change has been pretty swift in the last few years. I think it's been accelerated by the regulatory changes we're seeing – in terms of either affirming or excluding cyber coverage – with no 'grey' in between.

EH: There's also a lot of eyes looking at the cyber market to potentially pick up areas of exposure that historically fell within other product lines.

Are businesses beginning to think of cyber cover as 'essential' yet? Or is it viewed as an add-on/ luxury purchase?

EH: Regardless of size, if your business relies on IT to any degree – and you have even a minor incident – it acts as a wake-up call. People's understanding of how dependent they are on IT – and the implications if they can't access, or something happens to it, is growing. People are realising cyber cover is a pretty fundamental purchase.

AG: Many smaller clients recognise the value of the additional, value-added services they can access; such as training tools, compliance material, the virtual CISO service. It more than just paying a claim. It's about helping people reduce their risks and prepare.

And although it's not a legal requirement – like Motor cover for example – we have seen end clients requesting proof of cyber cover, a bit like they do with PI insurance.

How do you persuade people that cyber cover's an important purchase?

BM: There's an understandable degree of 'fear fatigue' right now, especially with the pandemic. So it's more a question of highlighting the services we provide – and asking the question: 'Who will you call if there's an issue?' A UK non-insured SME business is not going call the police to help with a ransomware incident. So how do they deal with it if they don't have a raft of companies on retainer to get them back up and running.

If an insurer can offer tools that enable businesses to get on top of the risk – which is frankly a bit of a mystery to a lot of businesses – and they can access resources to enable them to do so, then they'll respond positively to that.

AG: The message is a balance between: 'this is a very real threat with serious implications' and 'don't worry it can be mitigated; we will help you do that.' For us, having Datasafe as part of our offering is a huge positive; we believe Datasafe goes above and beyond other offerings by quite a long way. It provides more proactive tools to help clients manage risk, plus all the other free resources, which are more compliance-focused.

"Datasafe goes above and beyond other offerings by quite a long way."

Adelle Gruber

continued on next page

How does the cyber market look right now?

BM: It's at a crossroads. There's been explosive growth over the last decade, which has really accelerated in the last five years. Carriers have seen others writing this class of business – and heard stories of how profitable it's been.

The direct market's been fuelled by cheap and available reinsurance capacity. With the rise in loss activity and the severity and frequency of ransomware attacks, that's now beginning to turn the other way – and reinsurers are reassessing their appetites. Equally, as their books grow, insurers are having greater concerns around potential systemic exposures in their portfolio – ie a single incident potentially affecting multiple policies at any one time – and what the implications of that look like. So there's a inflection point at the moment.

AG: This isn't the first time we've seen a slew of big losses. The large data breaches around 2014 in particular saw a knee-jerk reaction from many high-profile cyber market players; pulling out, pulling capacity – and then re-entering the market further down the line. We didn't do that. Obviously, we looked at our underwriting portfolio and the risks in there, but we remained a stable market and continued to provide capacity in a prudent manner.

"We've always taken a case-by-case approach to everything we underwrite."

Georgia Drew

GD: And that aspect's been recognised by brokers; the fact that we've always taken a case-by-case approach to everything we underwrite. Brokers appreciate the fact that we're a stable market; we've had a consistent appetite over previous periods of loss activity – when we sought to underwrite our way through, rather than withdraw from writing risks.

continued on next page

thoughts on 2020 continued

Any thoughts on – or predictions for – 2021?

EH: The market's been flooded with quite naïve capacity in a soft market. Many players don't have the benefit of long experience in this class. Remember, we've been doing this since 2005. Now's the time for the experts to demonstrate their real value, especially when it comes to long-term client relationships.

CC: We'll continue to share the latest insights from our risk management peers and partners, and the wider market and help pass these learnings as quickly as possible to the end client.

BM: If an insured can demonstrate their resilience – their ability to manage risk – they're going to benefit. Anyone who can't do that is going to struggle. Risk selection will be key and that's certainly where our focus is going to be.

As a market leader, we have a chance to drive this where it needs to be driven – and become the changemakers. In terms of where things are heading this year, it's clear that market conditions are hardening; hence underwriting criteria, rates and coverage are all in the spotlight like never before. Other than that, the only thing I can predict for this year... is that it's going to be unpredictable.

in the spotlight

Congratulations to Brit's Senior Cyber Security Analyst Sunaina Aytan, who was recognised as one of the *#wonderwomenincyber* by Women in CyberSecurity (WiCyS) UK for 2021. Sunaina's work encouraging young girls into STEM subjects and cyber roles is truly inspirational – we're very proud to have her on our team.

news from datasafe

Ransomware and 'Smishing' attacks rising fast

Datasafe's Blog is currently featuring a Check Point report, which highlights a 45% increase in ransomware attacks on healthcare organizations globally in November and December. It's also drawing attention to SMS Phishing or 'smishing', which uses malicious text messages to steal information or access accounts. Security firm Proofpoint reports a 328% increase in smishing in the third quarter of 2020.

Stay current

Datasafe's Knowledge Center provides unlimited support to Brit's clients, with practical guidance on ransomware prevention, incident response and business continuity planning. Subscribing to Datasafe's mailings means clients also receive monthly updates on security issues and changes in regulation – as well as webinar invitations. Cyber alerts are issued whenever an imminent threat is discovered.