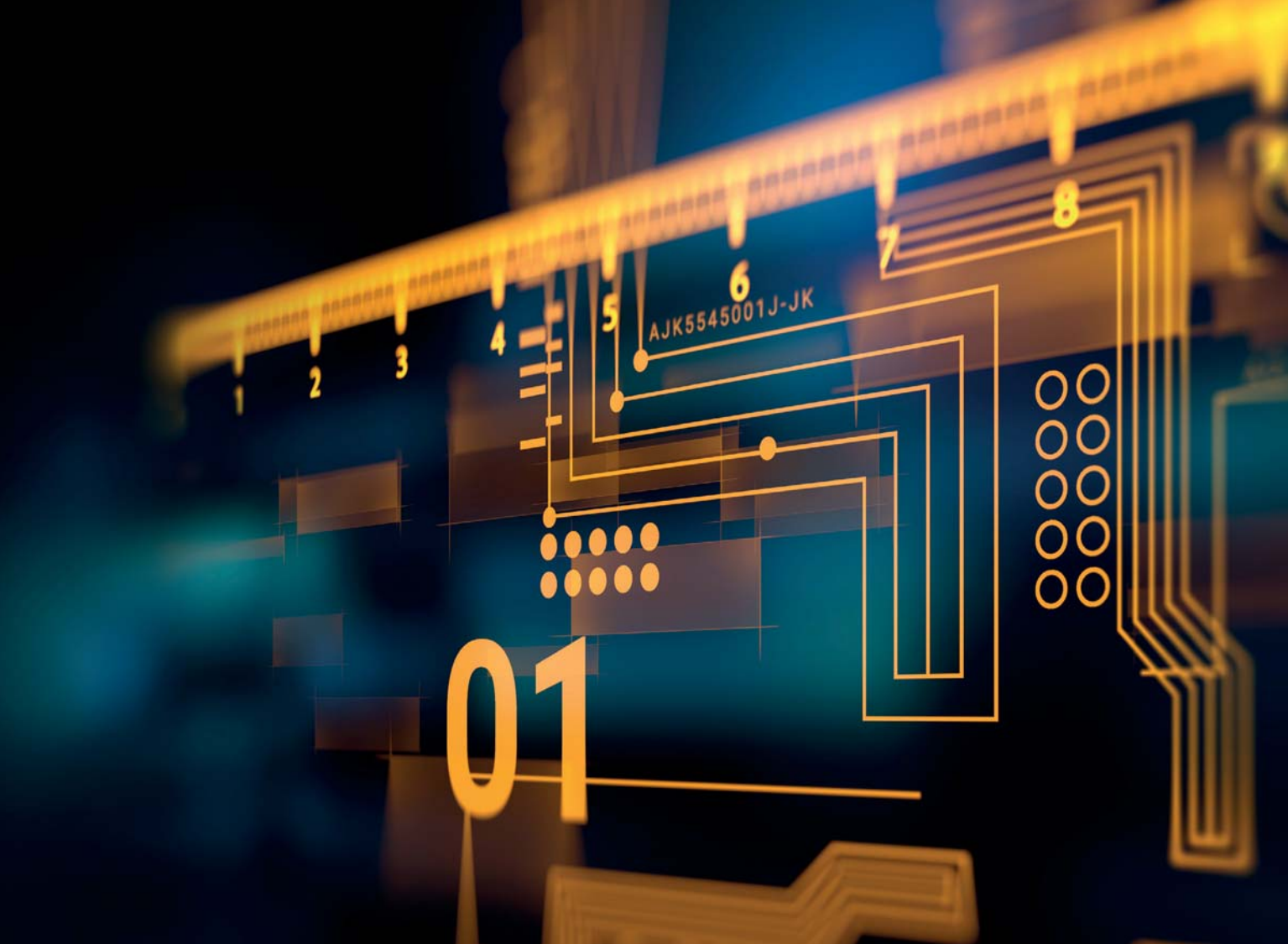

01

CYBER FOCUS

CYBER RISK FOCUS

Anup Seth, of Aon, discusses the company's recently implemented Cyber Captive Program, its breadth of coverage and conception as a solution to treat cyber risk as a standalone peril

Captive Review (CR): Talk us through the background of Aon's Cyber Captive Program – what decisions led to its implementation?

Anup Seth (AS): The genesis of this solution was borne out of the findings from the Aon cyber survey that we conducted in early 2016. This survey went out to over 200 risk managers, and we reviewed the findings and looked at the common themes – these proved rather startling.

Coverage limitations, in particular business interruption coverage arising from physical damage, was the top concern for participants. In addition, companies that had a physical-damage or bodily injury exposure, both first and third party, arising out of a cyber event felt that these exposures were not being addressed by the cyber policies currently available. The other interesting fact was that there was limited cyber risk assessment and only 25% of companies adhere to International Best Practices. These were the two most important findings that came out of this survey.

The other recurrent themes were – given that this is an emerging risk – inconsistent policy forms, limited understanding of how claims would be managed following a cyber-breach and low cyber insurance penetration – 60% of large companies do not buy cyber insurance.

These drivers led us towards designing and implementing the Aon Cyber Captive Program that includes four key components.

The first is the cyber resilience review that addresses the limited cyber risk assessment finding. This threat-based approach looks at the core assets and the key cyber threats that a company has and overlays the cyber-security controls to assess the strength of these controls against industry best practices. We also take a scenario-based approach, asking, what if this control fails; what would this loss look like? And such a scenario is drawn out, so there is a quantitative component to the cyber resilience report as well.

Anup Seth joined the firm as managing director of Aon Insurance Managers (Bermuda) Ltd. in April 2016 and is responsible for the overall leadership and oversight of the captive and insurance management operations in Bermuda. He has over 20 years of diversified international experience with a particular focus in providing specialty insurance solutions to multinational companies. Seth is a Fellow of the Institute of Actuaries (UK) and holds a BSc. Degree in Actuarial Science from The London School of Economics & Political Science."

The second is the policy form that provides comprehensive coverage for both non-physical and physical damage including business interruption arising from a cyber breach and is branded the Aon Cyber Enterprises Solutions form – the ACES form.

The third component is the risk transfer piece where we have aligned up to $400m of capacity from well-rated insurance companies that sits excess of a meaningful captive retention. There is also a pre-agreed cyber response team and panel of knowledgeable loss adjusters with a well-defined claims management process.

The final piece is the Cyber Risk Forum where we will invite the markets that are supporting us, clients that have bought the insurance, and claims adjusters to share knowledge.

We brought these components together that culminated in the Aon Cyber Captive Program.

CR: What is the current level of adoption regarding cyber insurance penetration?

AS: It largely depends on the industry. We found that if you look at the data holders – financial institutions, healthcare companies, and retail companies – they have quite a large penetration when it comes to cyber insurance. The survey found that 70% of companies that we classified as data holders were already buying some form of cyber insurance product, or had at least considered some form of cyber insurance protection.

In contrast, only 17% of companies in manufacturing had done any of the aforementioned. Part of that was because they thought the physical damage nature of their cyber exposure just wasn't being addressed – they hadn't even considered an insurance solution.

These were critical findings around driving the design of the ACES form. Looking at the cyber exposure spectrum, you have four quadrants – horizontally you have non-physical damage, and physical damage; vertically you have first-party and third-party liability – the challenge was to design a form that covered all four quadrants, and that's what we've done with the ACES form.

CR: What are the current biggest chal-

lenges and how is Aon positioned to respond to them?

AS: The first is around understanding your cyber-security controls and their strength, gathering the necessary data and getting the right people within the organisation to come together to understand what areas require further strengthening. The cyber resilience review brings all of this info together into one succinct report.

The second challenge when creating our program was in designing a solution for companies that had physical damage exposure arising out of a cyber event – this led us towards treating cyber as a separate, standalone peril. I think more companies need to be thinking along these lines.

It's not an extension of your property or casualty policy: we now treat cyber risk as a separate standalone peril, and hence it has its own form, and it covers those four quadrants of the cyber exposure spectrum.

The third challenge was around an understanding of the claims process. Through the acquisition of Stroz Friedberg inc., we have strengthened our cyber proposition considerably including a cyber response team.

A cyber breach isn't like any other breach; you can have a cyber breach and not even know about it. Once you're aware that something might have gone wrong, it's very important that you have the right response team to go into your company, to analyse and understand what type of breach you've had and to then respond to that breach accordingly to try to manage and mitigate the potential loss. Linked to this is the well-defined claims management process.

> "It's not an extension of your property or casualty policy: we now treat cyber risk as a separate standalone peril"

CR: **What is the ACES policy trigger and what other coverage does it afford?**

AS: All first-party coverage is provided on a losses occurring basis and all third-party liability is provided on a claims made basis – so there is a dual trigger to the policy.

In addition to property damage the ACES form provides cyber terrorism coverage, product liability coverage to address Internet of Things exposure and contingent network business interruption for IT vendors and the supply chain. We've also extended cover for any regulatory fines and penalties where insurable and arising out of a covered event. This is particularly relevant in the EU, where next year you have the EU General Data Protection Regulation coming in, effective 25 May 2018.

CR: **What steps do you take in the insurance process of this program?**

AS: The first step is the cyber resilience review that is conducted by the Aon Cyber Risk Consulting Practice. Once the resilience review is completed, the report goes to the client and then the client can decide whether they want to continue with the risk transfer solution, or they may find that – based on the report – that they'd like to remediate certain elements of their cyber-security controls.

Assuming they want to continue with the risk transfer, the next step is the design of the insurance program structure. This is determined by using the resilience review report and in particular the quantitative scenario-based results – looking at how much capacity the company should buy and the captive retention based on the company's risk appetite.

Once the insurance program structure is finalised, a dedicated broking team completes the insurance placement – we have a panel of pre-agreed insurers that have agreed and committed capacity of up to $400m on the ACES form.

Once the placement has been completed, we have a separate team within a company called Aon Underwriting Managers, and they are dedicated and work on behalf of the carriers. They work on matters such as issuing the policy, collecting premiums and administering any other policy endorsements that may be needed during the term of the policy.

CR: **What makes Aon's approach unique?**

AS: It's a combination of the cyber resilience review that offers both a qualitative and quantitative threat-based review, combined with the breadth of cover provided by the ACES form where all four quadrants are being protected. Finally, significant capacity provided in a timely manner on a consistent form to the insured. That is extremely valuable and is a truly unique solution in the marketplace at the moment.