THE NEXT GENERATION OF CYBER COVERAGE

The demand for cyber insurance is growing fast, and companies are increasingly seeking a bespoke solution that matches the specific needs of their industry. Jamie Bouloux, the chief executive officer of EmergIn Risk, part of RSG Underwriting Managers Europe Limited (RSGUM Europe), explains to Intelligent Insurer *how his firm is offering just that.*

In early August, a major US airline was forced to cancel more than 1,000 flights and delay thousands more after a power cut downed communications at its headquarters. The airline had not offered any estimates on the financial impact of the problem at the time of going to press, but analysts have suggested it could wipe at least $10 million off the company's operating income in the third quarter.

Although a power outage caused the initial problem, it triggered a series of knock-on challenges for the company's computer system which took several days to resolve. Analysts also commented on the vulnerabilities of an aging computer system for the company and the consequences when it goes wrong.

While this was not technically deemed a cyber attack or event in the way companies usually perceive them, the incident did, however, lead to a surge in demand from other airlines inquiring about cyber coverage.

Jamie Bouloux, the chief executive officer of EmergIn Risk, part of RSGUM Europe, says this is often how the fast-growing (but still embryonic in many ways) cyber market works.

"Many companies really understand the threat only when they see it happen in real terms in their sector," he says. "They see the true damage an event can do to their business, and they then look for the options available that can protect them against the consequences of that."

A GROWING OPPORTUNITY

EmergIn Risk, a managing general underwriter, was formed by RSGUM Europe in 2015 after Bouloux joined from managing general agent CFC. He previously worked at AIG with Peter McKenna, managing director of RSGUM Europe.

Bouloux describes cyber as one of the greatest opportunities for insurers at the moment as buyers and corporates grapple with these new and evolving risks, and new laws come into force in Europe stipulating the levels of protection some entities should have in place.

The cyber market is already estimated to be worth more than $2 billion annually, with an expectation for year-on-year growth in the non-US market of 70 percent. Global gross written premiums for cyber insurance are expected to reach $10 billion in 2020 compared with less than $2 billion in 2014, according to data compiled by Aon.

Bouloux believes that the way the segment is evolving is very sector-specific. The challenges and threats facing companies vary greatly, and as such, EmergIn Risk's offering is tailored by industry with the specific needs of those companies in mind.

A list of some of the key industries targeted by the company and the challenges they face can be seen below. He stresses that technological advances have made it easier to manage a wide range of information about customers, vendors, and employees. But this also means that virtually all businesses that use computer systems are to some extent vulnerable to costly exposures associated with system breaches.

"We help clients understand and cover the realities and practicalities of cyber attacks and the implications of systems failure," he says. "We especially focus on the non-physical business interruption element of this and the continuity issues companies face in the aftermath of an attack but also any type of system interruption event."

"This market clearly has huge growth potential, but it is also a process

"We especially focus on the non-physical business interruption element of this risk and the continuity issues companies face in the aftermath of an attack."

of educating people about the products available. The cyber market in the US is pretty well established but clients come to the market for different reasons. It is often the publicity associated with a large company having a specific problem that generates the interest."

BOOST IN EUROPE

Regulation has also driven much of the growth in this sector. In the US, for several years the onus has been on companies of a certain size to put in place measures to protect against such threats, and this has driven the growth in cyber insurance. Now, a similar process is expected in Europe.

New data privacy regulations to be introduced in 2018—the General Data Protection Regulation (GDPR), which will replace Directive 95/46/EC—are described by many as being much stronger, with much more significant ramifications than the US law.

It sets standards for data protection not only for companies within the EU but also for those outside the EU which are offering goods or services to EU data subjects. GDPR will carry fines of up to 4 percent of annual turnover for the mishandling of data breaches and stipulates that data breaches have to be reported within 72 hours.

Bouloux believes that these new regulations will drive cyber insurance take-up in Europe. He believes the nature of the demand may be different from that in the US and says the products his firm offers will be tweaked to take differing demand into account. It all adds to the growing understanding among buyers of what is available and their sophistication around how to best manage these risks.

This is why the organisation of EmergIn's offering around so-called industry verticals (designing each product to match a particular industry) is so effective. Bouloux says the company works with its clients to identify the potential operational and financial implications of cyber events and aligns with the clients' strategies to offset any unforeseen performance interruptions.

"Insurance solutions are developed by blending an understanding of a client's core business and helping to match any strategic planning and performance management initiatives with the perceived enterprise risk. This approach allows us to develop a balance of differentiated products and services which we are able to deploy to our target markets," he says.

Bouloux admits that the challenge remains for corporations to limit the risk to investment, performance and adaptability in the event of shocks to the enterprise. However, technology has forever changed the speed with which business enterprise risk can be derailed, with the potential for substantial financial and operational implications.

"We recognise why the next round of companies will come to market and buy this, and we have focused on their needs," he says.

"We have identified industry verticals in each sector and highlighted the concerns in each industry. This means we can give each client a customised solution. It is not a one-size-fits-all umbrella product but something very bespoke and suited to help address each client's unique needs." □

Jamie Bouloux is the chief executive officer of EmergIn Risk. He can be contacted at: jbouloux@emerginrisk.com; www.emerginrisk.com

SECTORS CURRENTLY TARGETED BY EMERGIN RISK

Healthcare has seen a big increase in cyber attacks. Estimates suggest that the global healthcare cybersecurity market will reach $10.85 billion by 2022, thanks to the rapidly increasing number of cyber attacks, regulatory and security compliance issues, and internal data leaks.

Criminal attacks against healthcare providers have more than doubled in the past five years, with the average data breach costing a hospital $2.1 million.

Hotels and restaurants have high levels of exposure to cyber threats because they collect vast amounts of private data from customers as a part of their day-to-day operations. Private data may be both personal (names, physical addresses, email addresses, passport details) and financial (credit cards and bank details).

Manufacturers are increasingly being targeted by not only traditional malicious parties such as hackers and cyber-criminals, but also by competing companies and nations engaged in corporate espionage. Motivations for these attacks range from money and revenge to competitive advantage and strategic disruption.

Oil and gas and utilities should all have security as a key priority yet nearly 70 percent of companies surveyed that are responsible for the world's power, water, and other critical functions have been hit by at least one security breach that led to the loss of confidential information or disruption of operations in the past 12 months. Now, these companies are investing in better protection on all fronts.

Retail has seen an increased number of extortion demands in recent years with several major breaches hitting the headlines. Further, as retailers become increasingly reliant on technology platforms, they are becoming exponentially exposed to these threats and the potential for system failures.

Airlines control huge volumes of customer data across extensive networks, operate one of the most complicated vendor and supplier networks of any industry, and are substantial contributors to national GDP both as employers and as transportation operators.

Despite being a $2 trillion industry, razor-thin margins mean that the operational or financial implications of a cyber event cause serious challenges for an airline operator.

Construction Upon acceptance of the initial tender and once the project has been scoped, the construction industry has developed technology to help with the planning, execution, and monitoring and tracking stages of the construction workflow. From the use of computer-aided design (CAD) to help develop architectural plans, to the use of building information modelling (BIM) for project management, system failures or security breaches of these systems could have not only an operational and financial implication, but reputational impact too.