impact

ACTIONABLE INSIGHT FOR BUSINESS LEADERS / **CYBER RISK** / MARCH 2016

CYBER RISK REGULATION:

FIRST LINE OF DEFENCE

Regulators and ratings agencies are beginning to take a much closer look at cyber risk, with a particular interest in data security and exposure management.

By Stuart Collins

Cyber risk is a hotly debated issue for insurers. On the one hand it offers a welcome source of new business and, as the world becomes more dependent on technology and data, cyber risk is destined to become a much bigger part of insurers' business. Yet it also comes with challenges, as insurers grapple with a lack of historical data and the threat of aggregation and systemic risks.

Against this backdrop, regulators and ratings agencies are becoming increasingly aware of the potential risks cyber presents to insurers' balance sheets and the industry's reputation, according to Derek Newton, principal and consulting actuary at Milliman in London.

"Cyber is a rapidly evolving area for insurers, but it is also an emerging challenge for regulators. We are already seeing regulators and ratings agencies show growing interest in insurers' cyber security and the exposures they are taking on their balance sheets as connected technology and the Internet become more and more relevant to their business," he says.

"As a result, insurers are likely to face greater reporting of cyber security risks and exposures in the not-too-distant future, while the way in which they use data, as well as its security and integrity, are likely to come under increasing scrutiny," he adds.

Protecting consumers, promoting growth

Regulators have a difficult task ahead, according to Christine Fleming, claims management consultant, Milliman. "Insurance supervisors and regulators will have to balance their primary concerns of consumer protection and solvency, with society's need for cyber risk transfer products," she says.

Adam Hamm, insurance commissioner for North Dakota, and chair of the National Association of Insurance Commissioners (NAIC) Cyber Security Task Force, explains: "Regulators do not want to stifle growth in cyber insurance. It has an important part to play in the US's cyber defence. We want the market to develop in the correct manner."

Kathryn Morgan, director of regulatory operations, Gibraltar Financial Services Commission, agrees: "Our statutory objective is to protect consumers. It is not the role of a regulator to predict or react in a knee-jerk fashion to innovation but to keep an eye on the market and develop new rules if needed."

On the role of the regulator in shaping the burgeoning cyber insurance market, Hamm continues: "As regulators, we would not look to micro manage the way insurers develop any line of business, so we would not want to dictate how they should grow cyber insurance.

We are already seeing regulators and ratings agencies show growing interest in insurers' cyber security and the exposures they are taking on their balance sheets as connected technology and the Internet become more and more relevant to their business.

Derek Newton, principal and consulting actuary, Milliman

"However, there is concern around insurers' ability to protect consumer data. And as the market grows, regulators will want to see that insurers understand the risks they are taking on and that they are able to make good on the policies they sell," he says.

Arguably, the NAIC has taken the lead among the world's insurance regulators, having been particularly active in addressing cyber security over the past year.

In 2014, the organisation established a Cyber Security Task Force, which has already made huge progress in promoting higher standards of cyber security, as well as moves to gather more information on insurers' cyber insurance activities and exposures.

Other regulators have been less visibly active. But that is not to say that cyber is not on their agendas. For example, the UK's Prudential Regulatory Authority (PRA) does not appear to have a specific regulatory policy for cyber risk, but it does have a programme regarding IT resilience and risk. During the summer of 2015, the Bank of England and the PRA conducted a survey of insurers' IT security, which included questions on whether they offer cyber insurance.

In its 2015/16 Business Plan, the UK's Financial Conduct Authority identified cyber crime as a risk to insurers, as well as warning that insurers need to ensure there is absolute clarity about what cyber insurance policies do and do not cover.

Targets of cyber crime

Regulators are concerned with both insurers' own cyber security, and the potential solvency risks associated with cyber-related exposures, according to Fleming. However, as the cyber insurance market is still relatively small, and exposures limited, the initial emphasis seems to be on improving cyber security, she says.

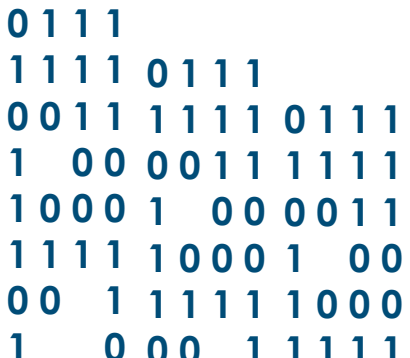
In the US, a number of healthcare insurers have been involved in massive data breaches, including the theft of as many as 80 million policyholders at Anthem, Inc. in January 2015.

In the UK, Royal Sun Alliance admitted in September 2015 that [some of] its bancassurance customers' personal details were compromised after a storage device was stolen from a data centre. In 2010, Zurich Insurance was fined £2.2m by the Information Commissioners Office after it lost 46,000 customer records.

Financial services companies, which hold large amounts of personal data on their customers, are attractive targets for cyber criminals, and this has not escaped the attention of regulators.

According to Morgan: "There is increased regulatory scrutiny of IT and cyber security risks for insurers. For all new licence applications in Gibraltar we review the company's IT systems, including those used to price risk and hold consumer data. We also conduct regular cyber security reviews based on the size of an organisation and the kind of work they do."

According to Alan Pereira, CIO, Gibraltar Financial Services Commission: "No company is safe from a cyber



attack. Organisations look to mitigate cyber risk but it can't be 100% eliminated."

The GFSC now looks closely at a regulated company's reliance on IT, the precautions it takes, access to data and business continuity planning, and whether they are following cyber security standards.

Pereira explains: "This is an issue that the Commission is taking very seriously. We require an annual statement of compliance which in the future will include details of cyber security. We'll also conduct ongoing regulatory monitoring – including supervisory visits – and are in the process of adding a review of cyber security."

Solvency II: A framework for cyber risk

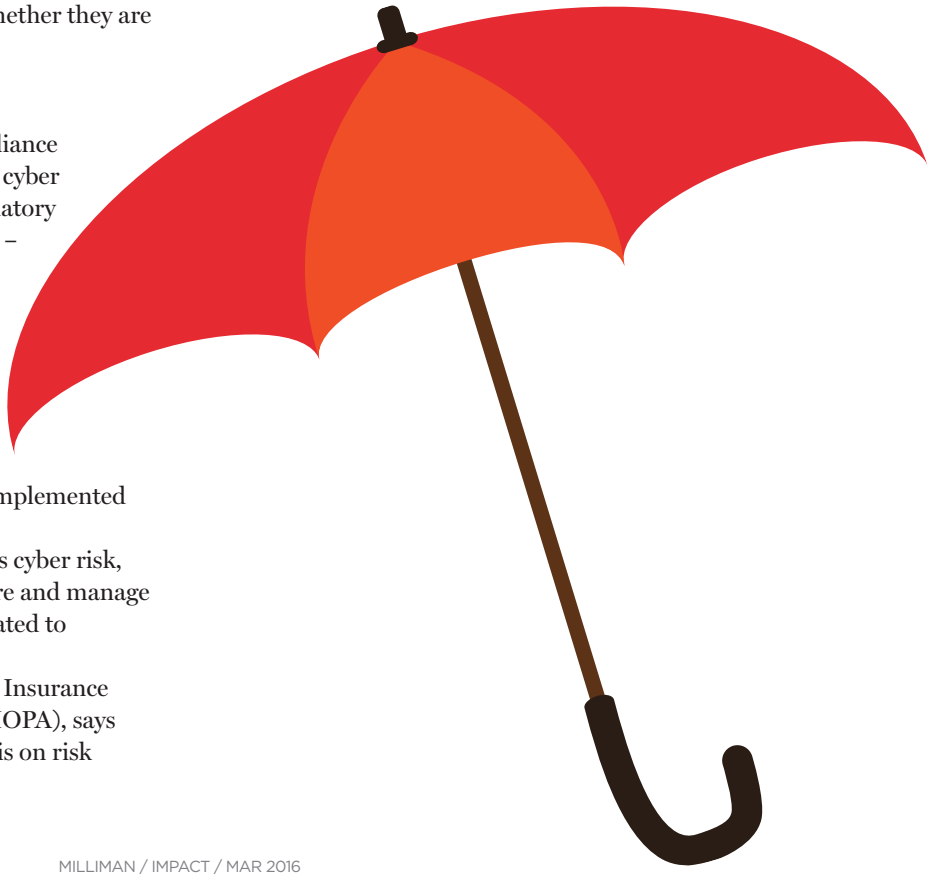
In Europe, regulators have been occupied with Solvency II, new capital and risk management rules which were implemented in January 2016.

Solvency II does not specifically address cyber risk, but it does provide a framework to capture and manage cyber exposures and operational risks related to cyber security.

The EU regulatory body, the European Insurance and Occupational Pensions Authority (EIOPA), says that Solvency II will increase the emphasis on risk management and will force insurers to consider both operational and underwriting risks in more detail, documenting the process and presenting it in a way that can be understood by regulators and other stakeholders.

EIOPA says: "In our view, cyber risk needs to be seen with regard to the undertaking's internal measures for protection of their data. Some relevant guidance is mentioned in EIOPA Solvency II Guidelines on System of Governance in the section 'risk management of operational risks'. Furthermore, the Own Risk and Solvency Assessment (ORSA) under Solvency II is the measure to assess all risks and to analyse any impact those risks may have on the solvency needs of the undertaking.

"In practice this means that – in its at-least-yearly ORSA – the undertaking has to assess all types of risks it



is exposed to and use scenarios and stress tests for each of its significant risks. According to the results of those stressed scenarios the undertaking should define its capital needs and its possible management actions for those significant risks."

In addition, EIOPA's Insurance & Reinsurance Stakeholder Group has established a sub-group to examine cyber risk and insurance. It is currently considering whether to formally look into the issue and how it might proceed.

International guidance forthcoming

Given the global nature of cyber risk, international regulatory guidance is likely to be developed in the future. According to Morgan: "The trend is in the direction of international regulatory guidance for cyber security. As technology creeps into more and more risks, regulators will need to keep abreast of the changing world and adapt."

Meanwhile, the International Association of Insurance Supervisors' (IAIS) recently stated: "Cyber crime is becoming more frequent, more sophisticated, and more widespread. It is therefore important that insurance regulators and supervisors, as well as insurers themselves, understand how cyber crime may affect the insurance sector, and take concrete steps to ensure development and implementation of best practices."

The IAIS Financial Crime Task Force (FCTF) has already started to draft an Issues Paper on Cyber-Crime Risks to the Insurance Sector. The paper is expected to be released for public consultation in mid-2016.

In addition, the FCTF recently increased its mandate to include "understanding developments in the cyber insurance market". It will produce a 'base-line' memorandum as well as regular updates.

Ratings agencies ahead of the game

Insurance ratings agencies are also starting to ask more questions of insurers' cyber security measures and their cyber insurance underwriting activities.

Fred Eslami, senior financial analyst at AM Best, says: "We are keenly interested to ensure that the insurance industry, in general, and our rated entities, in particular, are aware and prepared to face the challenges and threats that cyber attacks and data breaches impose upon them. We would like to see them recognising the risk and have plans to confront it as part of their overall risk management practices and ERM framework.

"For the companies issuing cyber insurance policies, the issue becomes more critical not only since the exposure is higher but also because cyber security risk has interdependencies, thus measuring and managing the aggregation of risk within cyber insurance portfolios becomes very critical."

Cyber security is now part of AM Best's annual rating review meetings. The ratings agency has also been conducting surveys and sending out various questionnaires to create a sense of awareness within the industry that reliable data is critical.

Via its annual Supplementary Ratings Questionnaire, AM Best asks rated insurers for information on the number of policies, total annual direct premiums,

> *We are interested to ensure that the insurance industry, in general, and our rated entities, in particular, are aware and prepared to face the challenges that cyber attacks and data breaches impose upon them. We would like to see them recognising the risk and have plans to confront it as part of their overall ERM framework.*
>
> Fred Eslami, senior financial analyst, AM Best

number of claims, and incurred losses and loss adjustment expenses, as well as their top three largest exposures.

Eslami adds: "As we obtain more information from our rated entities on the topic, we would be developing specific criteria relevant to cyber security – as we have for natural catastrophes and terrorism. This may take a few years; in the meantime, we continue with what I outlined above and gather information.

"At this time, when reliable consequence-oriented data and analytics are not readily available, we do not consider the risk as impacting any individual insurer's rating. But as more data and analytics become available, similar to natural catastrophes and terrorism, this risk would become relevant to and have an impact on an insurer's rating."

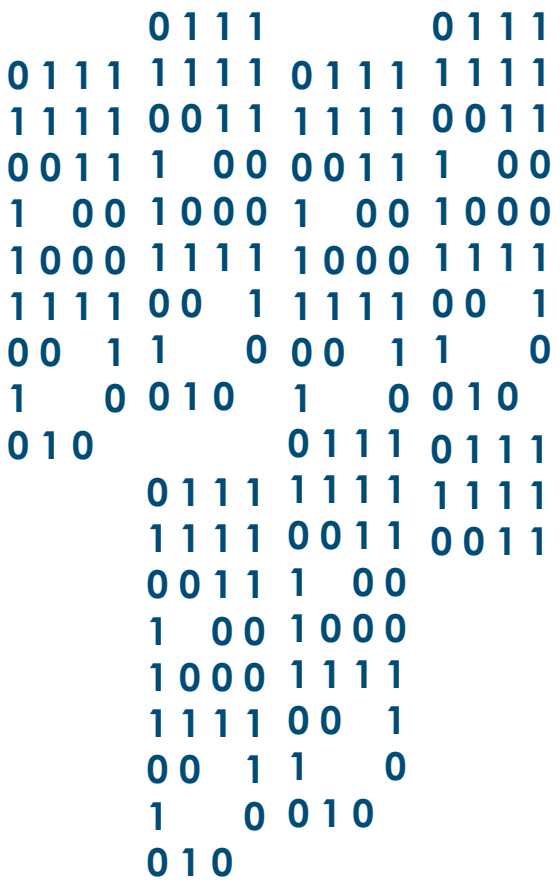
Ratings agency Fitch Ratings is also increasing its focus on cyber exposure monitoring and the protection purchased by rated insurers. Graham Coutts, Associate Director at the agency, says: "Insurers now collect and store more personal information about their clients than ever before. This will warrant an increase in attention paid to protection of data and response to breaches.

"Currently cyber risk is a relatively small line of business for most of our rated insurers. Fitch will continue to monitor this line closely due to its relative infancy and rapid growth."

Tougher laws

At the end of 2015, EU authorities finally reached agreement on EU data protection laws. The new laws, which are expected to be enforced in early 2018, are expected to significantly increase the penalties for a data breach or mishandling of personal data by European companies, as well as foreign companies dealing in personal data of EU citizens. The law applies to all sectors, including insurers.

As a result, it is likely that Europe will follow in the footsteps of the US, where tougher data protection laws have helped drive demand for cyber insurance. But more stringent EU data protection laws are just part of the story for insurers, says Newton.



"It is clear that cyber insurance and data protection are only going to grow in their relevance for insurance. Whether it's the use of 'big data', their own cyber security or an increase in cyber exposures on insurers' balance sheets, regulators are clearly taking more interest," says Newton.

Find out more

Christine Fleming
+1 781 213 6249
christine.fleming@milliman.com

Derek Newton
+44 20 7847 1606
derek.newton@milliman.com