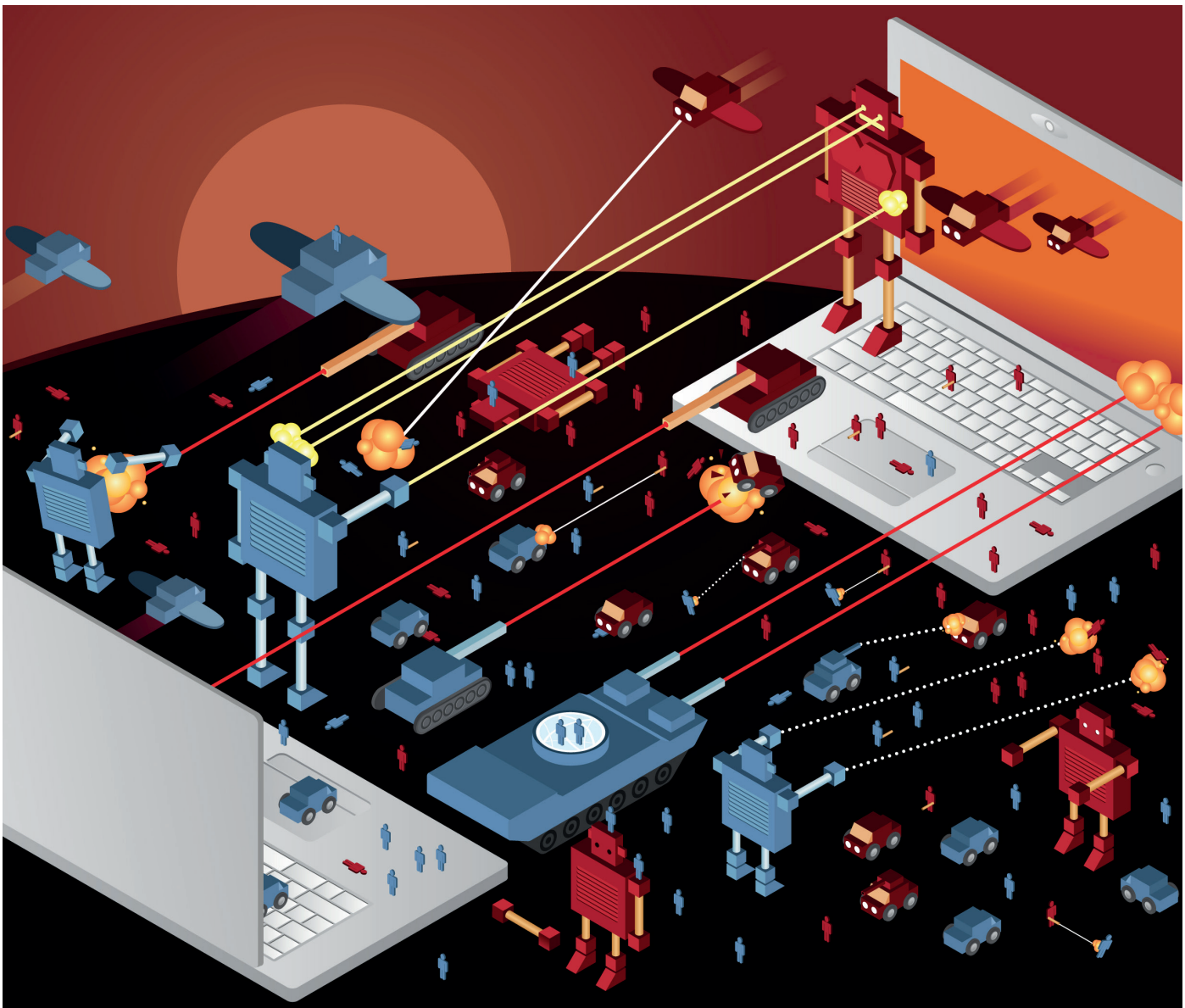
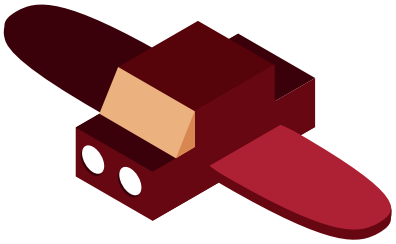
impact

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



BOLSTERING INSURERS' CYBER DEFENCES



At a time of unprecedented cyber attacks on insurers and an expanding cyber insurance market, US insurance supervisors have taken the lead in addressing insurers' cyber security risks

By Stuart Collins

Cyber security is a top priority for US insurance regulators, reflecting the rapid growth of the US cyber insurance market and the growing threat of cyber criminals to the sector.

2015 saw some of the biggest ever cyber attacks on US insurers. Data breaches at healthcare insurers Anthem, Premera Blue Cross, and CareFirst collectively resulted in the loss of personal data of more than 100 million US policyholders.

At the same time, the cyber insurance market is becoming increasingly relevant, both in terms of business written – it is currently one of the faster growing lines of insurance business, according to broker Marsh – and the potentially critical role insurance can play in helping business and society manage cyber security.

Regulatory agenda

US insurers, particularly those in the healthcare sector, have become a major target for cyber criminals. The breach at Anthem in January was one of the largest of any company in 2015.

Adam Hamm, insurance commissioner for North Dakota, and chair of the National Association of Insurance Commissioners (NAIC) Cyber Security Task Force, explains: "There is no question that insurers are being deliberately targeted by cyber criminals that see the industry as holding a treasure trove of information on hundreds of millions of Americans. I don't believe that we have crested the mountain of data breaches and I would expect that we will see many more.

"At present the US healthcare insurance sector has been the main target of cyber attacks aimed at the insurance sector, but the attacks are likely to spread to other insurers. Cyber criminals looking to access personal data need look no further than insurance companies – they are a potential one-stop shop for cyber-criminals."

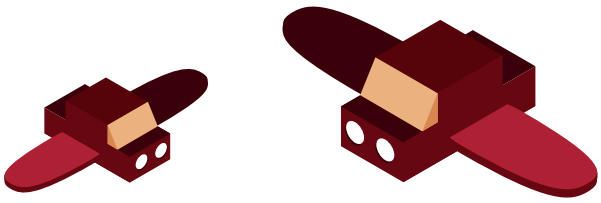
Cyber task force

Unsurprisingly, insurer cyber security has become an important issue for US regulators in recent years.

In the spring of 2015, the New York insurance supervisor wrote to more than 160 insurers encouraging them to view cyber security as an integral aspect of their overall risk management strategy. It also announced enhancements to the IT examination framework to include more detailed questions on an insurer's cyber security policies, protections, and procedures.

More significantly, the NAIC has engaged in a burst of activity, having taken the significant step of establishing a Cyber Task Force in November 2014.

Creating the task force demonstrates US insurance supervisors' commitment to addressing



The US healthcare insurance sector has been the main target of cyber attacks aimed at the insurance sector, but the attacks are likely to spread to other insurers. Cyber criminals looking to access personal data need look no further than insurance companies.

Adam Hamm, chair of the
NAIC Cyber Security Task Force

cyber security in the insurance sector, according to Christine Fleming, claims management consultant at Milliman in Boston.

State regulators already work with federal regulators to address cyber threats in the US. For example, the NAIC sits on the US Treasury Department's Financial and Banking Information Infrastructure Committee and on the Cybersecurity Forum for Independent and Executive Branch Regulators.

Although the creation of the task force coincided with a number of large high-profile attacks on US insurers, including Anthem, cyber security had been on the NAIC agenda since 2013.

According to Hamm: "There is concern among regulators over insurers' cyber security and the handling of breaches, and insurers selling cyber liability policies need to understand the risks they are undertaking. A number of Insurance Commissioners have deep concerns for solvency issues of insurers writing cyber insurance."

Regulatory actions

The task force's comprehensive work plan and timetable speaks volumes to the significance and urgency that US insurance supervisors and commissioners now place on cyber security, explains Fleming.

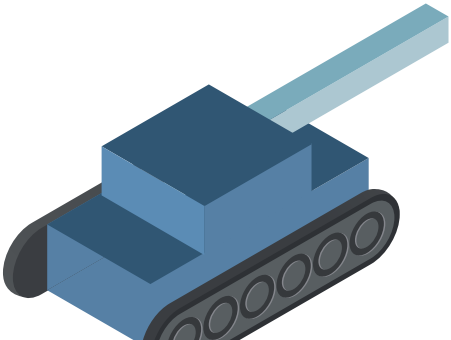
The task force is concerned with both the protection of consumer data held by insurers and improved monitoring of insurers cyber underwriting activities and exposures. During 2015, the NAIC embarked on four major work streams:

- Establishing guiding principles on cyber regulation
- Creating a Consumer Bill of Rights
- Modernising examination protocols to include cyber security
- Including a cyber security statement in insurers annual statement

As a first step, the NAIC enacted the Principles for Effective Cyber Security Insurance Regulatory Guidance in April, which set out the high-level regulatory strategy on insurer cyber security.

Compatible with National Institute of Standards and Technology (NIST) Cyber Security Framework, the guidance is a clear statement by the NAIC of the need for insurance supervisors to provide effective guidance to promote consumer protection.

If adopted by state insurance regulators, the principles would require US-domiciled insurers to identify cyber risks, implement breach response planning, and report cyber data, explains Fleming. They will also require



boards of insurers to oversee cyber risks, as well as incorporate cyber security into enterprise risk management processes, she says.

Another key plank was achieved on 14 October 2015 when the Cyber Security Taskforce adopted a Consumer Bill of Rights, concluding its second work stream. The Bill of Rights sets out the rights of insurance consumers, as well as the responsibilities of insurers, concerning personal data. However, the Bill of Rights is not legally binding and the actual rights of consumers are dependent on federal and state laws.

Cyber exams

The NAIC also tackles cyber security through its third work stream, proposing changes to the Financial Condition Examiners Handbook to a more robust investigation of an insurer's cyber security as part of periodic reviews of regulated insurers.

From 2016, insurance supervisors will conduct a new cyber security exam, reviewing individual insurer's cyber security protocols and looking to identify cyber risk.

Hamm explains: "The protocols are a 'deeper dive' into an insurer's cyber security protocols to identify potential breaches or any potential issues with the cyber liability policies they are selling."

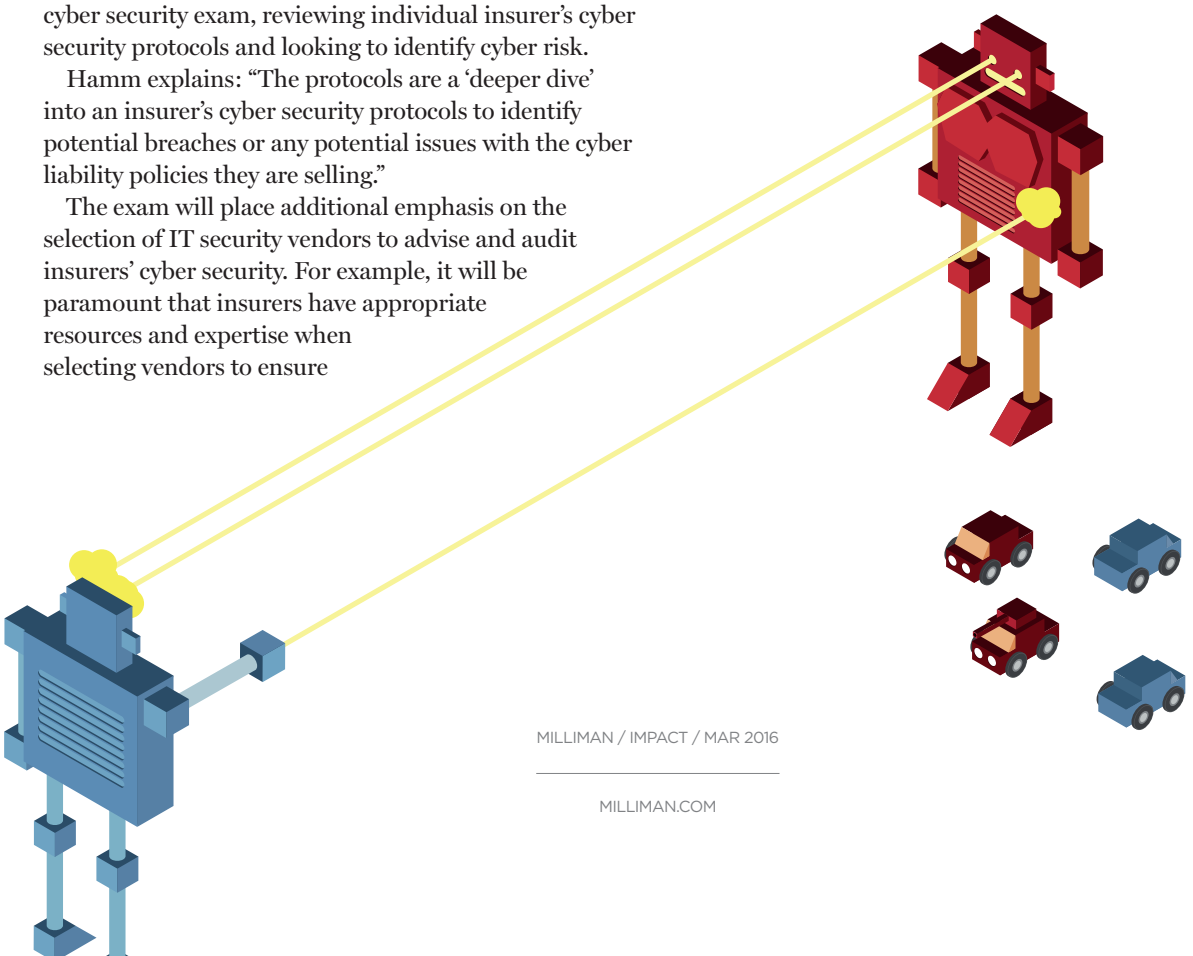
The exam will place additional emphasis on the selection of IT security vendors to advise and audit insurers' cyber security. For example, it will be paramount that insurers have appropriate resources and expertise when selecting vendors to ensure they are carrying out the correct types of cyber security audits and testing.

The cyber exam should also make companies take a more systematic approach to managing and testing their cyber security, which may best be achieved at present by following the NIST framework. The framework encourages companies to focus on five core functions to manage cyber security: Identify, Protect, Detect, Respond, and Recover.

Exposure data

In its fourth work stream the NAIC firmly turns its attention to insurer's cyber risk related to their underwriting activities. From 2016, US-domiciled insurers will need to complete a supplement to the annual statement, also known as the yellow book.

The supplement aims to collect information on insurers' exposure to cyber liabilities, as well as claims and premiums. Statistics on cyber insurance are



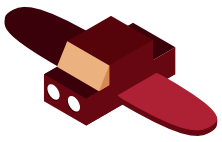
notoriously thin. Estimates of premium are just that – no one has a real handle on the size or make-up of the cyber insurance market.

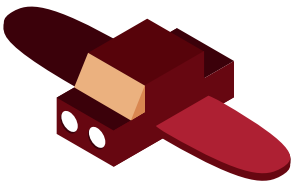
The NAIC will eventually produce aggregated statistics for the US cyber insurance market based on supplemental questions to regulatory filings. However, this will not include cyber insurance written on an excess and surplus lines basis – a sizable amount of US cyber insurance is thought to be written by Lloyd's.

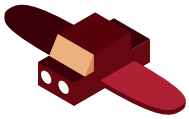
According to Hamm: "From late spring or early summer 2016, we will know the total premium for the cyber market, who is writing and how much they are writing, as well as trends in claims and market losses. We will no longer be working with estimates. Cyber will be brought into clearer focus."

The supplement and cyber exam should also prompt insurers to review underwriting guidelines and criteria related to cyber, especially as more data becomes available and as the cyber insurance market grows.

"Data transparency is clearly important, which is why the NAIC has taken steps to get a tree-top view of cyber risks. Cyber insurance is so new and continues to evolve on an almost daily basis. At the same time insurers do not have decades of data to rely on. The multiple of cyber exposures present a unique challenge to insurers," adds Hamm.





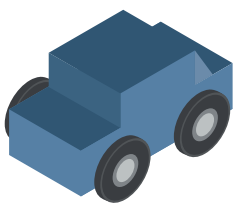


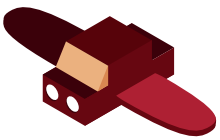
Although much of the information being requested by state insurance supervisors under the NAIC proposals will be readily available to insurers, they may also need to ask customers for additional information to monitor risk aggregation, says Fleming.

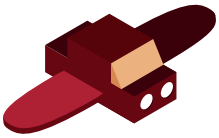
"It could be that US state regulators will drive insurance companies to think more deeply when underwriting cyber risks and to ask additional questions in submissions and renewal. At present, insurers carry out differing degrees of due diligence and ask varying degrees of information from policyholders," she says.

It could be that US state regulators will drive insurance companies to think more deeply when underwriting cyber risks and to ask additional questions in submissions and renewal. At present, insurers carry out differing degrees of due diligence and ask varying degrees of information from policyholders.

Christine Fleming, claims management consultant, Milliman







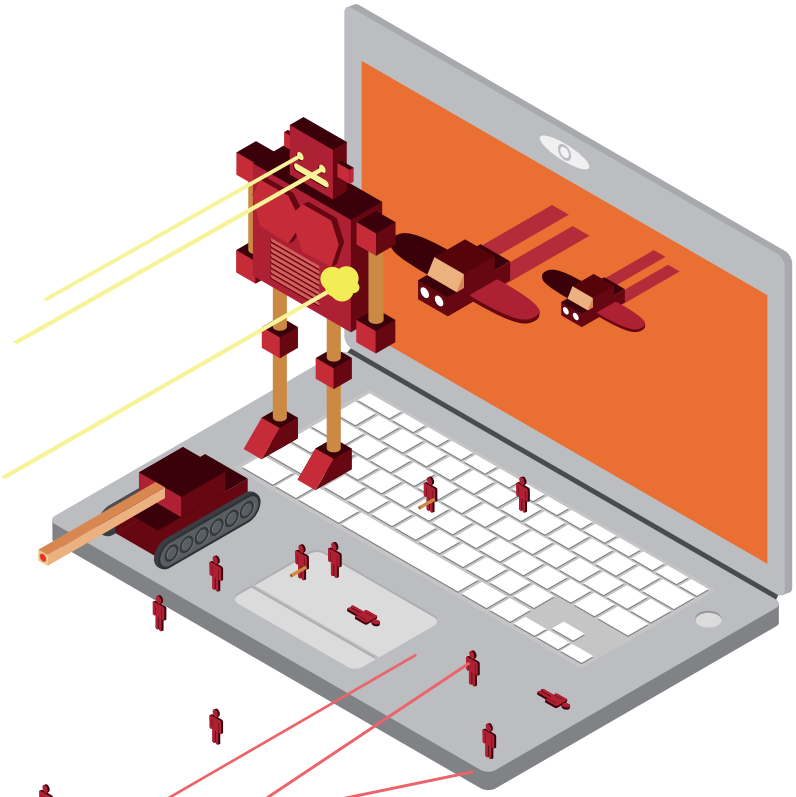
It is possible that insurers will pull back from certain risks as more data becomes available, continues Fleming. But long term, the accumulation of better data should give insurers more confidence in pricing and data management, facilitating growth in the cyber insurance market, she believes.

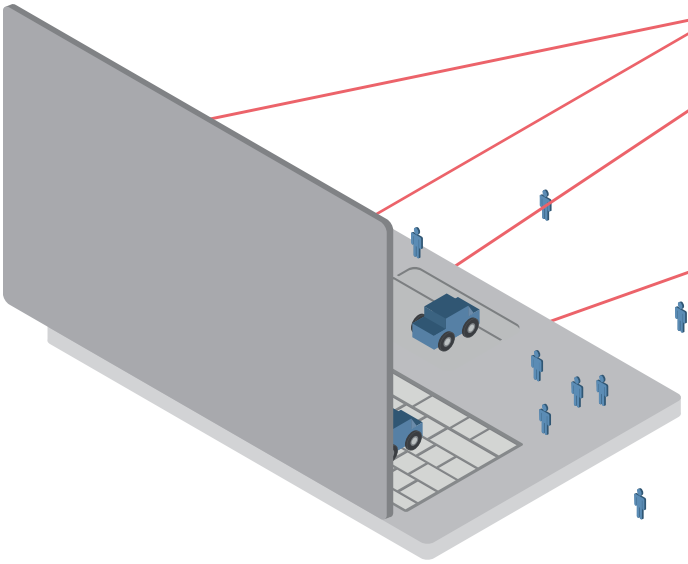
Having almost completed its 2015 work plan, the NAIC is now working on updating model laws with regard to cyber privacy and cyber security.

Although NAIC model laws are not compulsory, it is expected that most, if not all, states will adopt the new cyber security measures, although some states may wish to place additional requirements.

According to Hamm: "This year we will be busy updating NAIC model laws to implement the work on cyber so far, as well as potentially new changes.

"Once we get data and results of the exam protocols there may be additional work to do on cyber. We have tackled all the big issues, but there could still be more work to do in 2016 and beyond."





Find out more

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