Examples of cyber-resilience initiatives by national insurance associations

AUSTRIA

The Austrian insurance association (VVO) worked with insurance experts in Germany, Austria and Switzerland to develop non-binding master clauses for cyber insurance that were published in 2018. Alongside the non-binding clauses, the VVO has also developed a risk assessment questionnaire to help insurers assess the insurability of a client's cyber risk exposure. Most recently, the VVO has started gathering cyber insurance statistics, particularly information on premiums.

The VVO has been working with experts from the Austrian Road Safety Board (Kuratorium für Verkehrssicherheit (KfV)) to map cyber crime in Austria. The VVO and the KfV published the results of a survey of 500 SMEs in Austria in March 2017, which showed that 66% were affected by cyber crime in 2016. The VVO and the KfV also made recommendations on measures individuals can take to protect themselves against cyber attacks.

The VVO also works closely with the Austrian Federal Chamber of Commerce (WKÖ) on cybersecurity. In spring 2017, the WKÖ organised a roadshow in all nine Austrian provinces to raise SME awareness of cybersecurity and cyber insurance.

The WKÖ's online platform for cybersecurity features an online test to give SMEs detailed information on the level of IT security in their company. The questions focus on cyber threats that could disrupt the daily business practices of SMEs. On the WKÖ website there is also a checklist and risk analysis for SMEs on the implementation of the EU General Data Protection Regulation. A 24-hour cybersecurity hotline, offering three levels of assistance, is now available to WKÖ members free of charge.

BELGIUM

Assuralia, the Belgian insurance association, is a member of the Cyber Security Coalition. This coalition aims to fight cyber crime and has over 50 members from academia, public authorities and the private sector.

DENMARK

The Danish insurance association is a member of a forum created by the Danish police and the national centre for cyber crime. Participants in this group exchange information on a confidential basis on cyber attacks and receive information on national and international trends. The forum also organises conferences aimed at raising awareness of cyber risks.

FRANCE

The French insurance association (FFA) is part of GIP-ACYMA, a public-private partnership led by ANSSI (the French national agency for the security of information systems) and the Ministry of the Interior. The aim of the partnership is to create a national system of assistance for victims of cyber attacks. ACYMA targets individuals, companies and local authorities. Its objectives are to link victims of cyber attacks with local service providers via a digital platform, to launch prevention and awareness campaigns on digital security and to create a digital risk monitoring centre.

In May 2017, the FFA published a brochure that provides tips and information on how SMEs can anticipate and minimise the impact of cyber attacks.

GERMANY

In March 2017, the German insurance association (GDV) published non-binding wording for cyber insurance for SMEs. The model terms and conditions are designed for cross-sectoral, multi-line policies for cyber-risk insurance. They contain elements from traditional insurance products such as liability, property and employee fidelity.

The GDV also developed an online risk assessment tool, which can be used for free by potential commercial insurance buyers of all sizes to assess their own ICT security level and identify possible weaknesses.

The GDV is also collecting data on market developments relating to cyber insurance for commercial and private insurance customers.

NETHERLANDS

The Dutch association of insurers (VVN) has created a computer emergency response team for the insurance sector (i-CERT), a central service that informs and advises all affiliated insurers about cyber threats and incidents. i-CERT aims to improve the digital resilience of insurers, collect data on cyber incidents, limit the damage from cyber-security breaches, improve the provision of information on cyber security in the sector and increase the confidence of clients and stakeholders.

"Alert Online" is an annual awareness campaign by stakeholders from the public, academic and private sectors to make the Netherlands safer online. Over 170 stakeholders promote cyber-secure behaviour among Dutch consumers, the national and regional governments, companies (including SMEs), institutions and NGOs. Stakeholders organise events throughout the year, but the main activities of the campaign take place in October during European Cyber Security Month. "Alert Online" also publishes the results of its yearly cyber-security awareness survey in October. The VVN has been a partner in the campaign.

SPAIN

The Spanish insurance association (UNESPA), Cepreven (an independent technical standard-setting and certification body attached to UNESPA) and Cepyme (the Spanish confederation of small and medium enterprises) have developed a guide, "Cyber risk: its impact on SMEs", which details the measures to be adopted by organisations to protect themselves against computer attacks, mitigate the damage suffered when attacks occur and recover from them as soon as possible. The guide is free and available in digital and paper formats. UNESPA, Cepreven and Cepyme are promoting the guide at presentation days in different Spanish cities and through the media.

SWEDEN

A cooperation between the public and private sectors (including insurers) and led by the Bank of Sweden is developing scenarios for cyber incidents to increase the resilience of the financial sector.

SWITZERLAND

The cyber working group of the Swiss Insurance Association (SIA) focuses on the role of the state and data exchange, as well as on disaster scenarios and their impact. In parallel, the SIA has a number of workstreams that will have an impact on best practices in the medium term. For example, the SIA is part of the Swiss National Cyber Strategy (NCS2), to which it brings insurance-related topics.

UK

The National Cyber Security Centre operates a "Cyber Security Information Sharing Partnership" that allows the government and the private sector to exchange cyber-threat information in real time. The partnership was established in 2013 and the insurance industry is one of the largest participating sectors.

Insurance representatives, including the ABI, Lloyd's, the International Underwriting Association and the British Insurance Brokers' Association, also meet regularly with government officials through the Cyber Insurance Forum to discuss challenges facing cyber insurance.

Lloyd's has led the development of cyber scenarios with the aim of quantifying cyber risk aggregation. In 2017, Lloyd's and the company Cyence produced a report, "Counting the cost – Cyber exposure decoded", to provide insurers that write cyber coverage with two realistic and plausible scenarios. In 2015, Lloyd's and the Cambridge Centre for Risk Studies published a report, "Business blackout", which depicts a scenario in which hackers shut down parts of the US power grid, plunging 15 US states and Washington DC into darkness and leaving 93 million people without power.