Nicolas Jeanmart
Head of personal & general insurance, Insurance Europe

CYBER RISKS

A challenge and an opportunity

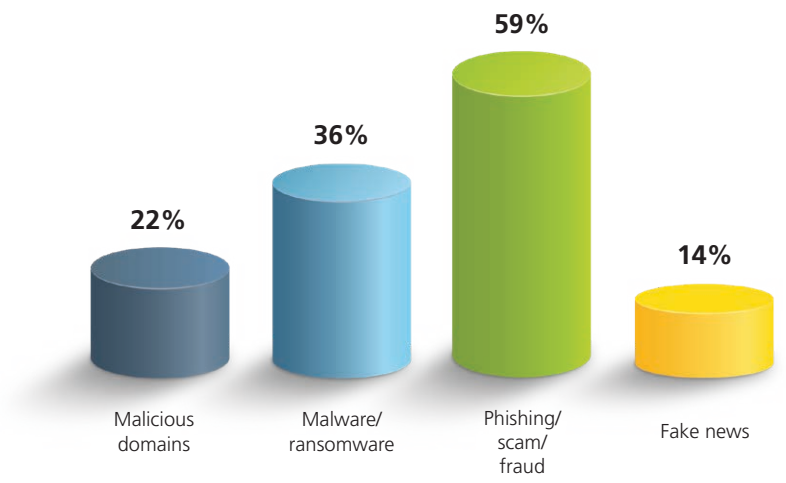
Insurers are both protectors and targets in the world of cyber risks

Many societal changes have been accelerated by the COVID-19 pandemic, but none more so than the digital transformation. Around the world, businesses large and small, including most insurers, have been forced to make the move to home-working in an effort to slow the spread of the coronavirus and protect their employees and customers, relying almost exclusively on digital technologies in order to stay in touch and keep operating. Both the capacity and security of IT systems have been brought sharply into focus, with Europol, the EU's law enforcement agency, reporting that the unprecedented shift in cyber activity has seen a corresponding rise in cyber criminality.

This comes at a time when insurance industry players and EU policymakers alike were already stepping up efforts to draw benefits from increasing digitalisation, while limiting as much as possible the associated risks.

On the side of EU policymakers, the European Commission of Ursula von der Leyen, which took office in December 2019 on a twin platform of sustainability and digitalisation, vowed to add to the patchwork of cybersecurity rules in the EU. Policymakers want to build on the General Data Protection Regulation (GDPR), which celebrated its second birthday in May 2020 (see p58), the Network and Information Security (NIS) Directive, which is heading for review at the end of 2020, and the Cybersecurity Act, which entered into force in June 2019. While these rules focus

% of Interpol countries reporting COVID-19-related cyber threats



Source: "COVID-19 Cybercrime Analysis Report", Interpol, August 2020

on businesses that process personal data (GDPR), undertake essential services (NIS) or want to certify their products, processes and services (Cybersecurity Act), policymakers are now looking directly at financial institutions, seeking to address a perceived gap in their cybersecurity and increase the "digital operational resilience" of the sector as a whole.

With this in mind, the Commission consulted on a "framework" of new information and communications technology (ICT) rules aimed at bringing all aspects of the cybersecurity of the financial sector together under one piece of legislation. The Commission's goal is to establish requirements for all organisations across the financial sector, including insurers, in the areas of:

- ICT risk management
- Incident-reporting and information-sharing
- Stress-testing of ICT infrastructure
- Oversight of critical ICT third-party service providers

No one-size-fits-all approach

If adopted, the Commission's envisaged approach could change the landscape of cyber incident management, reporting and prevention across the EU financial sector. For Insurance Europe, it is key in this process to keep in mind that the financial sector is not uniform, as organisations differ greatly — not only in their type, size and profile, but also in the risks to which they are exposed and the systems and services that need to be protected and maintained. European insurers are therefore calling for a risk-based approach to cyber resilience, distinguishing between critical and less critical functions.

Alignment of rules

The Commission is not the only body with its eye on strengthening the cybersecurity of the insurance industry, as EIOPA will also publish sector-specific guidelines on ICT security and governance for the insurance industry. Insurance Europe has therefore called for alignment between the various EU-level initiatives to avoid any multiplication of obligations and requirements placed on organisations — all of which are intended to achieve the same goal. For this same reason, insurers would also like reporting requirements, under the GDPR, the NIS Directive (where relevant) and a future Digital Operational Resilience Framework, to be streamlined.

Two sides of the same coin

In the area of cybersecurity, the (re)insurance industry occupies a unique position, both as a sector that finds itself increasingly vulnerable to cyber attacks and as a business that can offer protection through a range of cyber insurance products and services.

Insurance Europe's cyber policy recommendations

DO

- Promote awareness-raising, which is key to increasing cyber resilience
- Support public-private cooperation on catastrophic risks
- Urge member states to act to increase cybersecurity
- Support efforts to make cyber-incident data available

DON'T

- Introduce premature standardisation, which can harm both customers and insurers
- Introduce mandatory insurance for cyber risks, which would be counterproductive

Cyber insurance has a key role to play in helping European businesses to become more cyber-resilient, offering many different services, both before and after an incident. Cyber insurance can also enhance the competitiveness of European businesses — helping to foster an appetite for innovation in areas of digital technology by providing a safety net so that, if things go wrong, they do not bear the risks alone.

It is better for businesses, though, if they have less need to avail themselves of damage cover or *ex-post* support, and insurers also have a key role to play in prevention — making businesses aware of their possible exposures by assessing their "IT hygiene".

During the COVID-19 pandemic, insurers have been active in the area of prevention, and several national associations have run campaigns to raise awareness of the risks associated with home-working, including the increased vulnerability of businesses due to use of private home networks and computers. Indeed, the pandemic has confirmed the importance of cyber resilience for businesses of all sizes (see chart opposite) and has highlighted the key role of insurers in the prevention, mitigation and transfer of cyber risk.

Policy "dos and don'ts"

Though traditionally seen to be lagging behind its sister market in the US, the European cyber insurance market is growing year-on-year, thus contributing to increasing Europe's cyber resilience. In October 2019, Insurance Europe published a booklet containing recommendations — "dos and don'ts" (see box above) — for policymakers when looking to further encourage the growth of the market.

Among these recommendations, European insurers call for support from policymakers across the EU in the area of awareness-raising, public-private cooperation and increased access to data on cyber incidents.

On the subject of data, Insurance Europe is in favour of leveraging on existing data on cyber incidents, such as incident data gathered under the GDPR and the NIS Directive — and possible future data to be gathered under the Digital Operational Resilience Framework. To this end, back in 2018, Insurance Europe already developed a template for breach notifications under the GDPR, which would allow for data to be gathered in an anonymised but sufficiently granular format to be of use to the insurance industry.

In terms of policy "don'ts", European insurers advise against the introduction of premature standardisation or mandatory insurance for cyber risks, as this would hamper a market that is growing but is yet to reach its full maturity.