

## Cyber insurers are part of the solution to ransomware, finds Geneva Association report

- New Geneva Association report highlights the **important role of private re/insurers**, alongside governments, in boosting society's resilience to ransomware and ensuring the full benefits of digitalisation can be realised.
- The report explores the significant **value add of cyber insurance** beyond risk transfer, amid ongoing debate on whether to ban ransom payments or associated insurance coverage.
- Governments should do more to **counter ransomware attacks**: disrupt cybercriminal business models, fight illicit use of cryptocurrencies and promote cyber hygiene throughout business and society.

**ZURICH, 20 July 2022** – The frequency of ransomware attacks, a form of cyber extortion, is increasing, along with the size and nature of ransom demands. Cybercriminals are deploying more sophisticated approaches to target governments, businesses and individuals, with serious and costly effects. The growth of the ransomware-as-a-service (RaaS) business model has also enabled threat actors with limited technical skills to launch highly disruptive attacks.

Cyber insurance provides vital financial protection and operational support in the event of an attack, but ransomware has contributed to the recent deterioration in cyber insurers' underwriting performance. Ransomware accounted for 75% of all cyber insurance claims in 2020 (AM Best) and is also likely to have been the costliest loss event category in 2021 (WTW).

The Geneva Association's report analyses the complex policy issues surrounding ransomware and possible solutions to counter this epidemic in cybercrime, including the contribution of insurance to boosting firms' cyber resilience.

The report's key messages include the following:

- **Cyber insurance does more than provide cover for ransoms:** Cyber insurance may also cover first- and third-party losses incurred by victims of ransomware (e.g. business interruption, data and system recovery, forensics and legal assistance), as well as arrange expert support in managing incidents. Insurance also helps organisations identify and address cybersecurity vulnerabilities and adopt better risk prevention in a fast-changing landscape.
- **Banning ransom payments would be a blunt, potentially ineffective policy instrument:** An outright ban on the payment of ransoms or their reimbursement by re/insurers could backfire by driving transactions underground and encouraging ransomware attackers to engage in new, more malicious forms of extortion.

- **Governments and regulators must do more to counter ransomware attacks:** Public policies should be aimed at deterring ransomware attacks, disrupting cybercriminals' business models and illicit use of cryptocurrencies, and better preparing organisations for intrusion.

Managing Director of The Geneva Association, **Jad Ariss**, said: "With ransomware we see an example of the important 'prevention and mitigation' role insurers play as risk managers. They control a critical lever with their ability to incentivise customers to maintain strong cybersecurity controls and standards, helping to reduce firms' vulnerability to attack and boost their cyber resilience. Governments and regulators have their levers, too, and as our report highlights, they need to rein in the illegal use of cryptocurrencies and do more to ensure information exchange about incidents as well as improve international cooperation among law enforcement."

The Geneva Association's Director of Cyber and Evolving Liability and author of the report, **Darren Pain**, said: "The ransomware landscape is now highly evolved and sophisticated, especially with the development of ransomware-as-a-service (Raas). Such ransomware attacks are driving significant increases in insurance claims and, as a consequence, premiums. Would banning ransom payments be a viable solution? According to our study, insurance companies do not think so. Prohibiting ransom payments or their reimbursement by insurers would likely drive transactions underground, forfeiting the ability of the authorities to record and analyse incidents and prosecute criminals. Furthermore, the last thing we should do is take steps that might discourage smaller firms from taking out cyber insurance, the benefits of which go well beyond reimbursing ransoms."

*The Geneva Association is the only global association of insurance companies; its members are insurance and reinsurance CEOs. Based on rigorous research conducted in collaboration with its members, academic institutions and multilateral organisations, The Geneva Association investigates key risk areas that are likely to impact the insurance industry, develops recommendations and provides a platform for stakeholders to discuss them. In total, the companies of Geneva Association members are headquartered in 26 countries around the world; manage USD 21 trillion in assets; employ more than 2.5 million people; and protect 2.6 billion people.*

<https://www.genevaassociation.org/news/press-releases/insurers-part-of-solution-to-ransomware>

ENDS

Contact:

Pamela Corn

Director of Communications

+41 44 200 49 96

[pamela\\_corn@genevaassociation.org](mailto:pamela_corn@genevaassociation.org)