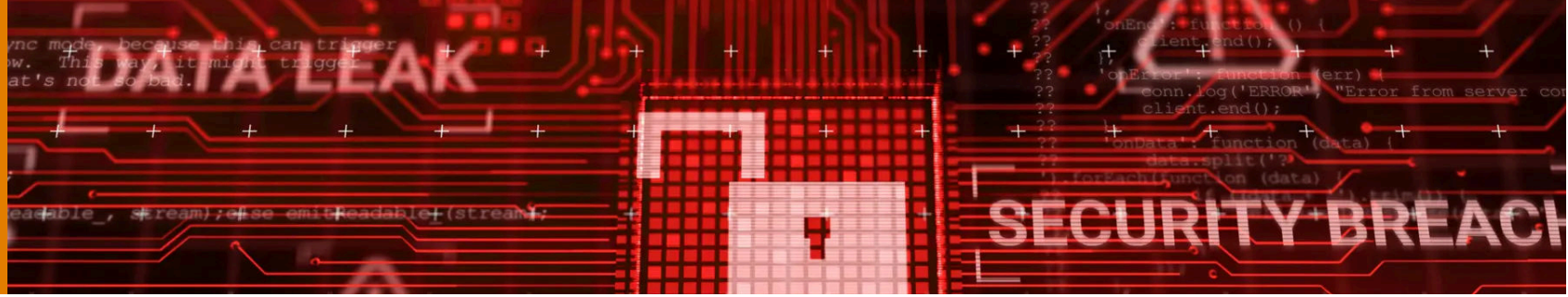


Into the breach

GFIA’s recent study analyses the growth in cyber risk and makes recommendations for tackling it

By Robert Gordon, chair of the GFIA Cyber Risks Working Group

The increased presence of technology in our lives has created great opportunities. From remote working to the fast and efficient delivery of goods and services and beyond, technology makes positive contributions to lives and businesses.

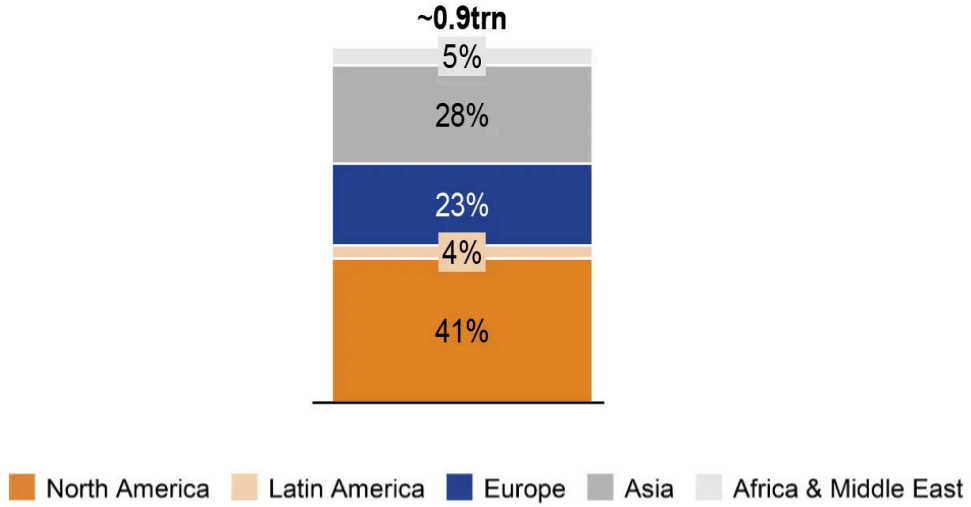
Yet it also exposes individuals and organisations to cyber attacks. And as the use of technology continues to grow, so will the need for individuals and businesses to protect themselves from cyber risk.

In its recent study, “Global protection gaps and recommendations for bridging them”, (see box for more details), GFIA identified an estimated gap of nearly US$0.9 trillion a year in the protection needed against cyber risks.

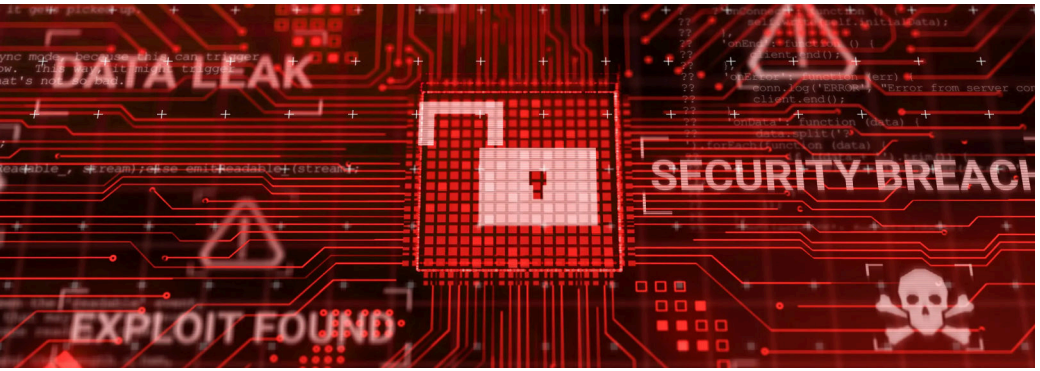
What is GFIA’s protection gaps study?

Annual cyber protection gap (US$trn) and geographic split

2-minute watch: Robert Gordon on the cyber protection gap



This cyber protection gap is defined as the difference between first-order economic losses from cyber attacks, which total around US$0.95 trillion, and the losses currently covered by insurance, which amount to around US$0.06 trillion.



“First-order economic losses are US$0.95trn but the losses currently covered by insurance are only US$0.06trn.”

First-order losses include, for example, damage to industrial facilities, bodily injury, software replacement costs and ransom payments. Second-order losses, such as reputational damage, are a frequent result of cyber attacks, but they are difficult to quantify and were therefore not included in the calculation.

These figures show that insurers currently only cover a fraction of global cyber risks, with the USA being the world’s largest cyber insurance market and accounting for roughly 70% of all gross written premiums.

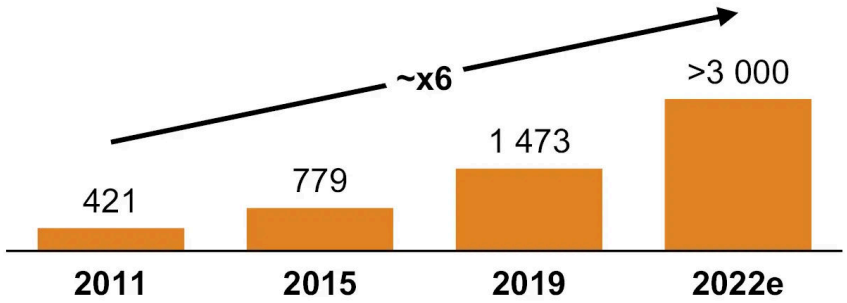
Cyber risks are very hard to insure, notably because of the difficulty of modelling future claims due to the evolving nature of the risks and to accumulation risk, when different risks are combined in one loss event. These, and other factors, such as the need to build adequate expertise, explain why many insurance companies currently do not offer cyber-risk solutions.

Insurance capacity is increasing, but so are risks

Although the number of companies that do offer cyber insurance is growing across the world, the rise in losses in recent years has led many of them to reassess how to create resilient, sustainable, long-term cyber coverage. For instance, some insurers decreased their cyber-insurance capacity and/or reduced coverage limits per policy. There has also been an increase in the focus on the security that companies need to have in place in order to be considered for insurance coverage.

Nevertheless, overall capacity is growing globally; forecast to reach anywhere from US$13 billion to US$25 billion by 2025. However, despite this increase in supply, the rapid pace of digitalisation and the resulting increase in vulnerability to attacks means that the protection gap is unlikely to be closed in the near future. SMEs, with less to spend on security measures, are particularly vulnerable.

Number of cyber breaches with >50 000 files lost



Trends influencing the number of cyber attacks include:

- Commercialisation of and innovation in cyber attacks
  AI is now widely used by attackers to send phishing emails, while the provision of ransomware as a commercial service and cryptocurrencies have significantly reduced the cost of carrying out ransomware attacks. Conversely, organisations that deploy AI and automation in their security seem more resilient.
- Growth in the Internet of Things
  As more “things” become connected, new vulnerabilities and risks are arising.
- Growth in remote working
  To take just one example, there was a 148% spike in ransomware attacks during the first wave of the COVID-19 pandemic.
- Political instability
  Geopolitical conflict frequently triggers spikes in cyber attacks.

As well as the increase in the number of attacks, the costs per incident are also increasing — up by 10% between 2020 and 2021 alone.

Solutions are available

The current level of losses may look grim, but risk awareness is rising and tools and strategies already exist to reduce the dangers and make cyber risks more insurable. Prevention measures can potentially decrease an organisation's cyber risks by 70%. They can also eliminate 80−90% of the costs of an incident, if it occurs. Risk training is particularly effective, as human error is a contributing factor in approximately 95% of all cyber incidents. And, as far back as 2016, a survey by Swiss Re found that over two-thirds of cyber insurance providers already offered or planned to offer prevention services to their clients.

Narrowing cyber protection gaps has to be the shared responsibility of all. Insurers can, and are, taking steps to address them — by running awareness campaigns and incentivising prevention, for instance. However, closing the gaps will also require actions from policymakers to create environments in which risks can be managed and mitigated. GFIA has five recommendations of ways in which policymakers can have the largest potential impact on reducing cyber protection gaps (with their local suitability depending, of course, on each country's regulatory environment):

“Narrowing cyber protection gaps has to be the shared responsibility of all.”

DO

- Promote awareness of cyber risk and incentivise cyber-risk prevention
  Actions can include: collaborating with the insurance industry to provide resources and education; developing guidance, standards and best practices; and educating consumers and businesses about the role of cyber insurance.
- Promote improved cyber resilience, particularly among critical infrastructure firms and assets
  Possible actions include: adopting mandatory cybersecurity requirements; imposing higher cybersecurity standards on critical national infrastructure; considering a cyber insurance programme to mitigate the impacts of a catastrophic cyber event; and bolstering efforts to catch and prosecute cyber attackers.
- Create a harmonised cyber-incident reporting framework
  Work with the insurance industry to develop an effective incident-reporting regime that prioritises existing standards and harmonises the framework as much as possible with those of other jurisdictions.
- Facilitate the sharing of aggregated data with insurers and academics for risk modelling and mitigation.
  Analyses show that the introduction and enforcement of cyber-risk reporting legislation in the USA, for example, correlates with the growth of its cyber insurance market.

DON'T

- Do not prohibit ransomware payments
  Making ransomware payments illegal could discourage the reporting of attacks and penalise victims.

GFIA hopes that its study will inform discussions between insurers and policymakers on the best ways to reduce exposures to cyber risks.

Further reading:

- *“Global protection gaps and recommendations for bridging them”, GFIA, March 2023*

Robert Gordon

American Property Casualty Insurance Association

Print version

What is GFIA's protection gaps study?

Gaps in protection have major consequences for the well-being and financial resilience of individuals, businesses and society. The world's insurers have a responsibility to understand and communicate the risks that will have the most impact on people's lives. That is why GFIA commissioned the first-ever study to identify and quantify the largest global protection gaps and to make recommendations for how policymakers and insurers can work together to close them.

The study, "Global protection gaps and recommendations for bridging them", was published in March 2023. It identified four gaps that have the most impact on people's lives due to their size, global presence, impact on livelihoods and expected growth. They are: gaps in pension provision (US$1trn); cyber-risk protection (US$0.9trn); health cover (US$0.8trn); and protection against natural catastrophes (US$0.1trn).