GFIA

GLOBAL FEDERATION OF INSURANCE ASSOCIATIONS

Global protection gaps and recommendations for bridging them

March 2023

Report extract:
Cyber protection gap

II. Executive summary

"The pace of change has never been this fast — yet it will never be this slow again." This statement by Canadian prime minister Justin Trudeau in 2018 describes the pace at which megatrends disrupt the world we live in, implying high levels of change and uncertainty for both individuals and organisations.

Four megatrends are particularly relevant given their global economic relevance and their impact on human lives:

- **Climate change**, which impacts lives and livelihoods around the globe. The World Economic Forum estimates it will create costs equivalent to between 4% and 18% of global GDP by 2050 if no adequate preventive actions are taken.
- **Technological acceleration** and the use of data, which has increased exponentially over recent years, with the amount of data stored globally expected to reach an unprecedented 180 zettabytes[2] by 2025.
- Changing **demographics** leading to ageing populations (in the USA, for example, 21% of the population is expected to be above 65 by 2030, up from 17% in 2020). At the same time, GDP productivity will shift towards emerging countries, which will account for 35% of global GDP in 2040, up from 25% in 2020.
- Disruptive developments in **macroeconomics and politics**, which will increase the level of uncertainty and volatility across the globe as supply-chain disruptions, inflation and other developments hit economies worldwide (eg, inflation in Europe was at almost 10% in July 2022 compared to 2.5% in the previous year).

These megatrends also change today's risk landscape by reinforcing existing risks and creating new ones, increasing the vulnerability of both individuals and organisations. Among the newly emerging risk areas are cyber risk, supply-chain disruptions and environmental liabilities.

The risk landscape impacts:

- individuals (such as pensions, health, mobility and homes, as well as disability, morbidity and death);
- businesses (such as business continuity); or,
- both individuals and businesses (namely personal and business liability, property, financial markets, natural catastrophes (natcat) and war and terrorism).

The risks vary in terms of economic relevance, speed of growth, direct impact on human lives (whether they cause major hardship or death) and insurability (whether private insurers or public systems can at least partially cover them).

Of these risks, **pensions, cyber, health** and **natcat** stand out due to their growing economic importance, impact on human lives and insurability. Exploring the current protection landscape and analysing the protection gaps related to these risks is particularly relevant due to their substantial economic and human impact.

While the insurance industry can contribute to reducing these protection gaps when the underlying risks are insurable, a single stakeholder group alone cannot narrow the gaps. Close collaboration between private and public stakeholders is necessary, as governments and other public entities can help build the appropriate regulatory environment, create fiscal incentives or conduct public awareness and prevention campaigns, among other actions.

Below we describe these four protection gaps in more detail and summarise the possible levers that private and public stakeholders can use to reduce them. We end this Executive summary with GFIA's own recommendations to policymakers for reducing the protection gaps in cyber, pensions and natcat.

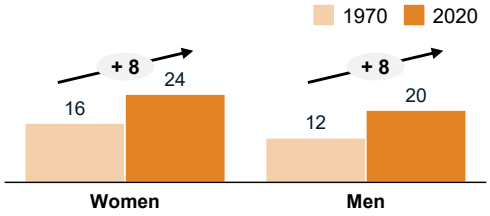
2 10^{21} bytes or a trillion gigabytes

Four major protection gaps

Accelerated by current trends

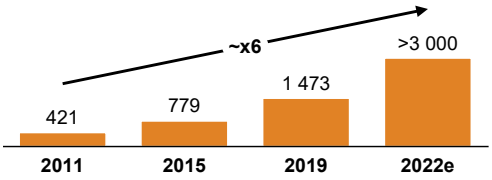
Pension

Expected life years after labour market exit (OECD countries)



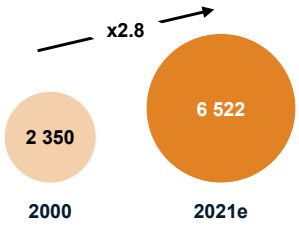
Cyber

Number of breaches with >50 000 files lost



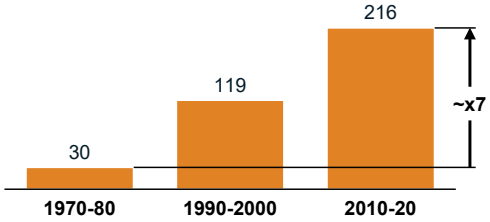
Health

Health spending[1] in OECD countries (US$ per capita)

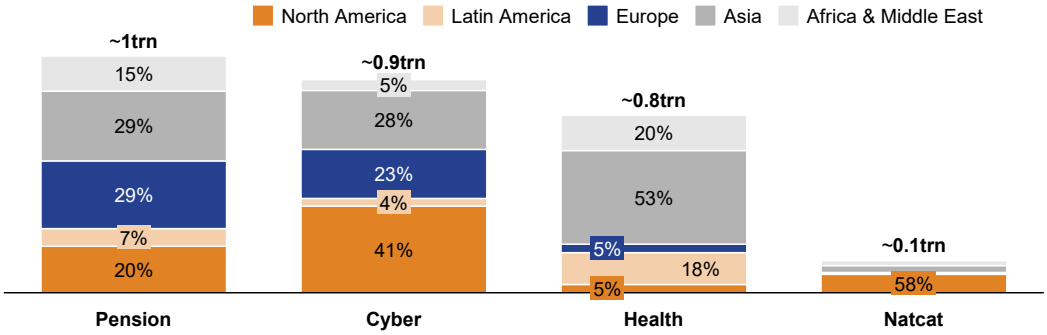


Natcat

Average annual natcat losses per decade[2] (US$bn)



Annual protection gaps (US$trn) and geographic split



Pension	Cyber	Health	Natcat
Cumulative gap of US$51trn after deducting pay-as-you-go, converted into an annuity of US$1trn p.a. with a 1% interest rate over 40 years	First-order cyber losses (US$0.95trn) minus paid cyber claims (US$0.06trn)	Stressful out-of-pocket spending[3] only. Gap could reach up to US$4.0trn if spending avoided due to financial constraints is included	~60% of natcat losses not insured between 2011 and 2020

e = estimate

1. Including personal healthcare (curative care, rehabilitative care, long-term care, ancillary services and medical goods) and collective services (prevention and public health services and health administration), excluding investments
2. Events caused by natural forces triggering insurance policies, eg, floods, storms, earthquakes, droughts, forest fires, frost, hail and tsunamis
3. Spending by individuals that puts pressure on their finances

Cyber protection gap — risks are growing in frequency, severity and variety

The increasing presence of technology and exponential use of data in almost all aspects of life is a global phenomenon. While it might create many opportunities — from remote working and driverless cars to the seamless delivery and automated dispersal of fertilisers in agriculture — it has also significantly increased exposure to cyber risks.

The number, severity and types of cyber attacks have grown globally. Insurers and other private and public stakeholders have started addressing the increasing need for cybersecurity and related financial protection. However, the market is still relatively nascent, especially in terms of the evolving regulatory environment and the developing awareness among individuals and organisations of cybersecurity and prevention measures and in terms of the rapidly evolving nature of both the technological landscape and the nature of the threats (such as the emergence of ransomware attacks in recent years).

We define the cyber protection gap as the difference between the total economic exposure of first-order losses from cyber attacks (eg, damaged industrial facilities, bodily injury, software replacement and ransom payments) and the losses currently covered (approximated with the global premium volume for cyber insurance). Second-order losses that are a frequently observed, indirect consequence of cyber attacks (eg, reputational damage) are difficult to quantify and are not included to ensure comparability with the other protection gaps.

Insurers currently only cover approximately US$6bn in paid claims annually, with the USA being the largest cyber insurance market, accounting for roughly 70% of global cyber GWP. Although increased loss ratios in recent years have made insurers reconsider their cyber underwriting policies and risk appetite, the supply of cyber insurance in terms of GWP is growing and is expected to reach US$13-25bn by 2025. With the increase in technology and digitisation, annual economic losses from cyber incidents are estimated at over US$0.9trn, having seen substantial growth in 2020 as a result of the COVID-19 pandemic. However, due to the small share of insured losses, the estimated protection gap remains at approximately US$0.9trn.

Although the supply of cyber insurance is expected to grow, it is unlikely that the cyber protection gap will be closed soon due to the small share of insured losses today and the rapid speed of digitisation, making businesses increasingly vulnerable to cyber attacks. Furthermore, since they are dependent on the regulatory environment (eg, incident-reporting standards) and public cybersecurity infrastructure, insurers will not be able to narrow the cyber protection gap alone (particularly for potentially systemic cyber risks), meaning private and public stakeholders need to collaborate to address the fast-growing cyber protection gap. Individuals and organisations need to seek cyber protection and proactively engage in prevention.

Various potential levers exist for private and public stakeholders to use to address the protection gap. These include: incentivising and supporting prevention; conducting awareness campaigns; developing incident-reporting frameworks; and fostering adaptation measures.

- The incentivisation and support of prevention measures can potentially decrease the cyber risk of an organisation by 70%. For example, insurers offer *ex-ante* risk-mitigation services in the form of risk engineering and include financial incentives in their policy clauses, which can reduce an organisation's premiums or deductibles if security measures are implemented.

- Awareness campaigns by both public and private stakeholders are a way to address the protection gap by educating individuals about cyber insurance and explaining the importance of security measures.

- Public policies that define a clear regulatory incident-reporting framework with necessary security could facilitate risk modelling by insurers. For example, analyses show that the introduction and enforcement of the cyber-incident reporting legislation in the USA correlates with the growth of its cyber insurance market, thus potentially reducing the protection gap.

- Public stakeholders may also foster prevention and adaptation measures that help reduce the number and severity of cyber incidents. For example, there are several existing initiatives fostering IT skills among professionals. In addition, regulatory frameworks and requirements supporting prevention and adaptation, such as minimum cybersecurity standards, have improved cybersecurity. The establishment of cyber-attack response units is another lever employed by governments.

The suitability of these levers for addressing the cyber protection gap needs to be assessed individually for each country, as countries may have different regulatory environments for cyber risks and insurance.

GFIA recommendations for policymakers

Introduction

This report has been produced by GFIA to promote greater understanding of the largest protection gaps faced by individuals, businesses and societies globally. Later chapters look into these gaps in more detail, examine the drivers and provide an overview of the wide range of potential levers that could be considered as ways to help reduce each of the gaps. The range of potential levers covered in later chapters include both actions that insurers can take and actions the public sector can take. The potential levers identified for policymakers have pros and cons — some can have unintended consequences and others may work in some jurisdictions but not in others. Nevertheless, all the levers have been included in the report to give as complete an overview as possible.

In this section of the report, GFIA focuses on its own recommendations for policymakers because insurers' ability to help reduce protection gaps is dependent on appropriate actions being taken by regional, national and supranational policymakers. It is they who can design and create the environments in which risks can be best managed and mitigated and so allow insurers to play their key role.

The following sets of recommendations represent "dos" and "don'ts" with which the global insurance industry considers policymakers can have the largest potential impact across the world in helping to address protection gaps.

Recommendations to policymakers for narrowing the cyber protection gap

Promote awareness of cyber risk and incentivise cyber-risk prevention.

- Collaborate with the insurance industry to provide resources and education about the risks of operating online — particularly for consumers and small businesses, as these groups tend to underestimate the risks — as well as to develop easy-to-understand steps that they can take to reduce their cyber exposure.
- Develop guidance on what constitutes good cybersecurity for IT systems, as this would help businesses develop security measures in a cost-effective manner and may positively impact insurance premiums.
- Develop cybersecurity standards and best practices for users to follow and actively support the private sector through public awareness campaigns and training programmes.
- Educate consumers and businesses on the role of cyber insurance as a mechanism of risk transfer and a method of helping businesses recover in the event of a cyber breach.

Promote an improved landscape of cyber resilience, particularly among critical infrastructure firms and assets.

- Consider adopting mandatory requirements on cybersecurity, especially for key economic sectors, subject to existing regional and national frameworks.
- Ensure that the agencies and contractors with whom governments and regulators do business evaluate their cybersecurity according to uniform and regularly updated standards. Look to adopt model systems that impose higher cybersecurity standards on critical national infrastructure, based on its level of strategic importance, so that it is minimally impacted by cyber events and system-wide breaches.
- Continue to evaluate, in partnership with the insurance industry, the merits of a cyber insurance programme to mitigate the impacts of a catastrophic cyber event. Any programme should take into account the downstream catastrophic damage that could result from a massive cyber event.
- Bolster efforts to pursue and prosecute those who are perpetrating cyber attacks.

Create a harmonised cyber-incident reporting framework to gain better insight into the frequency and severity of major incidents.

- Work with the insurance industry to develop a cyber-incident reporting framework to encourage targeted organisations to report incidents including ransomware, phishing, email compromise and other attacks. Such a framework should support automation and ongoing analytics.
- In any effort to design an effective incident-reporting regime, focus on creating a mechanism that is minimally onerous and avoids delaying the delivery of essential services. This is especially important in the immediate aftermath of a cyber attack.
- Prioritise the re-use of existing standards, so any new initiatives should encourage best practices and minimise, to the extent possible, the creation of new requirements.
- Harmonise cyber-incident reporting frameworks as much as possible across jurisdictions, and ensure participation and requirements are tailored and fit for purpose.

Facilitate the sharing of aggregated data with insurers and academics for the purpose of risk modelling and risk mitigation.

- Effective cyber-risk modelling can help quantify the risks associated with a system-wide cyber incident and measure accumulation risk. Additionally, risk modelling can help identify whether a cyber backstop is required.
- Jointly with the insurance industry, determine: the information that can be provided and will be most helpful for risk modelling; the best way to collect this data; who should have access to the data; and what limitations should be placed on how the data can be used/disclosed.
- Implement safeguards in any data-sharing effort to adequately address security and confidentiality concerns.

Do not prohibit ransomware payments.

- Making ransomware payments illegal could discourage the reporting of ransomware attacks and penalise victims. It may also leave businesses unable to deal with the outcome or provide the necessary assistance to customers, who may also be impacted. In some cases, the costs involved could result in the insolvency of the targeted company.
- In the event of a ransomware payment, encourage the targeted organisations to report the incident to the relevant authorities. This ensures that the payment of a ransom is clearly recorded and that the judicial authorities are informed of criminal activity. It also increases the availability of data about ransomware events.

IV. Cyber protection gap

Risks are growing in frequency, severity and variety

For a summary of this chapter, see the Executive Summary, "Cyber protection gap", p8. And for GFIA's recommendations for closing the cyber protection gap, see the Executive Summary, "GFIA recommendations", p15.

Cyber is among the top three risks on the minds of business executives[46]. The frequency, severity and complexity of attacks are rising, and they are exacerbated by large-scale digitalisation and the shift of traditional business activities to online operations. As employees worldwide shifted to remote working in 2020 because of the COVID-19 pandemic so did organised crime, with the commercialisation of cyber attacks severely disrupting businesses. The increasing geopolitical instability observed in 2022 is expected to bring with it a new and stronger wave of incidents, while technology and automation accelerate the need for cybersecurity, making it a top priority for businesses. At the same time, the supply side — cyber insurance coverage — is still an evolving market, with 2020 losses challenging insurers to find new ways of servicing the increasing demand. Beyond insurers, other private and public stakeholders have started tackling this growing gap.

The Geneva Association defines cyber risk as "any risk emerging from the use of information and communications technology that compromises the confidentiality, availability, or integrity of data or services"[47]. Cyber losses are commonly grouped as first-order losses (bodily injury, physical asset damage, financial theft and fraud, cyber ransom and extortion, business interruption, data and software loss, regulatory and legal defence, and incident response costs) and second-order losses (reputational damage and lost business). When estimating cyber-attack losses, we only include first-order losses to make them comparable with the other risks considered in this report.

Cyber, a multifaceted risk

Ransomware and data breaches are most common cyber attacks

First, a definition is needed of the types of cyber incidents and resulting cyber losses that are included in cyber risk. The attack method creates the incident type: ransomware (23%) and data breaches (13%) were the most frequent types in 2020, followed by vulnerability exploitation (10%) (Figure 4)[48]. These incidents lead to various operational disruptions, such as data confidentiality breaches (of own and third-party data), operational technology or network communication malfunctions, inadvertent disruptions of third-party systems and cyber fraud or theft (eg, illegitimate financial transfers).

The losses resulting from disruptions can be incurred directly by the entity under attack (first party) or by the organisation's clients and suppliers (third party). In 2020, approximately 25% of all cyber-incident claims in the USA for both stand-alone (covering one specific risk) and packaged (covering several risks) policies were related to third-party losses[49].

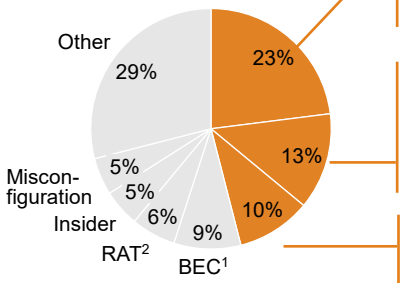
The incidents above can be accidental or driven by malice. Attackers include organised crime and state-affiliated and unaffiliated entities. Organised crime, which had seen a decline between

46 "Allianz Risk Barometer 2021", Allianz Global Corporate & Specialty, January 2021
47 Martin Eling and Werner Schnell, "Ten key questions on cyber risk and cyber risk insurance", The Geneva Association, November 2016
48 "IBM X-Force Threat Intelligence Index 2021", IBM Corporation, February 2021
49 "US cyber market update: 2020 US cyber insurance profits and performance", Aon, June 2021

2017 and 2019, came back with full force in 2020 and 2021 as the commercialisation of ransomware occurred. Organised crime was responsible for approximately 40% of incidents in 2018[50], a share that increased to roughly 80% of breaches in 2020[51]. In terms of motive, financial motives prevail and have been growing steadily. In 2020, they were behind approximately 85% of breaches versus roughly 70% in 2018. The second most common motive was espionage (10-15% percent of cases in 2020)[52].

Figure 4: Ransomware, data breaches & vulnerability exploitation were top three cyber incidents in 2020

Cyber incidents by methodology — 2020



Ransomware

Malware that employs encryption to hold victim's information to ransom. Often designed to spread across the whole system and can thus quickly paralyse an entire organisation.

Data breach

Incident in which information is stolen from a system without the knowledge of its owner. Victims usually suffer reputational damage and financial losses due to a perceived "betrayal of trust".

Server access/exploit

Exploit in which malicious players take advantage of a software vulnerability or security flaw. When used, it allows an intruder to remotely access a network and gain elevated privileges or move deeper into the network.

1. Business email compromise: scam targeting companies that conduct wire transfers and have suppliers abroad
2. Remote access trojan: type of malware, a tool used to gain full access/remote control of a user's system so that attackers can silently browse applications and files and bypass common security such as firewalls, intrusion detection systems and authentication controls

Sources: IBM; Trend Micro

Insurers cover US$6bn in cyber losses annually

Based on the definitions above, we estimated the supply side, ie, how much is currently covered by insurance and trends influencing this coverage.

Global insured cyber losses around US$6bn in 2021

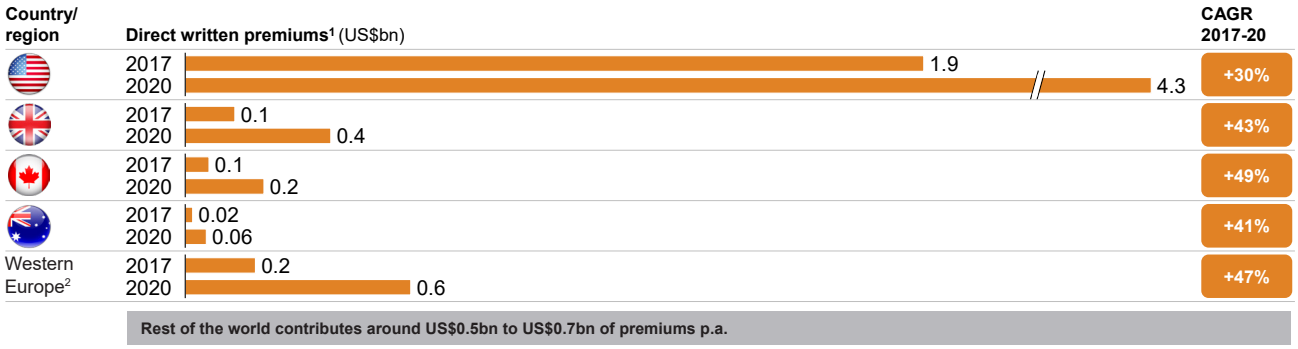
Potential insured losses can be estimated based on the cyber GWP value and reported loss ratios. According to Munich Re, global cyber insurance premiums reached US$9.2bn at the beginning of 2022[53] and have been growing at 30-50% per annum in its main markets (Figure 5). If USA loss ratios of 65% are taken as an approximation of global loss ratios, the volume of total insured losses paid by insurers can be estimated at approximately US$6bn in 2021[54].

The USA is the most developed cyber insurance market, with approximately 70% of global cyber GWP. This is followed by the UK and western European markets. All markets have exhibited strong annual growth of more than 30% since 2017. According to a McKinsey survey, cyber insurance penetration and the average premium per policy show strong growth in the USA and the UK. Penetration, measured as a share of businesses (both SMEs and corporations) covered by cyber insurance, increased from 7% to 13% in the USA and from 2% to 6% in the UK from 2017 to 2020[55]. Penetration in both markets is growing among both SMEs and large

50 2019 Data Breach Investigations Report, Verizon, 2019
51 2021 Data Breach Investigations Report, Verizon, 2021
52 Ibid
53 "Cyber insurance: Risks and trends 2022", Munich Re, 16 March 2022
54 "US cyber insurance sees rapid premium growth, declining loss ratios", Fitch Ratings, 13 April 2022
55 McKinsey survey, 2021

corporations, with a higher increase among SMEs in the UK and among large corporations in the USA. The average premium per policy also grew 3-5% annually from 2017 to 2020 in both markets.

Figure 5: Cyber is fast-growing service line

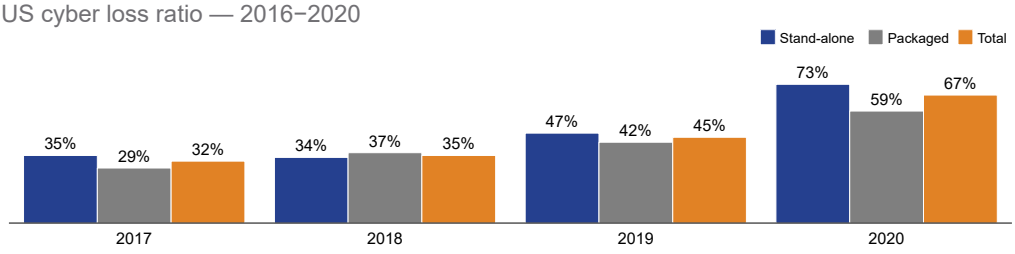


1. Does not include cover for businesses owned or operated by single individuals
2. Primarily Germany and France

Sources: S&P Capital IQ Pro; MSA Research

Figure 6: Cyber loss ratio massively increased in 2020

US cyber loss ratio — 2016–2020



Source: AON; Fitch Ratings

105% spike in ransomware attacks in 2020

Losses rose continuously from 2017 to 2020, with a spike in 2020 primarily driven by a sharp increase in ransomware attacks (105% year-on-year growth)[56]. In the USA, market loss ratios[57] increased from 32% in 2017 to 67% in 2020 (Figure 6). The combined ratio has been rising accordingly — in the USA, it increased from 75% in 2019[58] to approximately 95% in 2020[59].

The rise in losses revealed the limitations of existing models for cyber risk, with some insurers reassessing their approach to create resilient, sustainable, long-term cyber coverage for their customers. Some insurers decreased the capacity they allocated to cyber, reduced coverage limits per policy for existing and new clients, and limited the cyber insurance included in traditional policies. For example:

- Approximately 80% of 200 commercial insurers from the USA expected they would limit cyber insurance capacity in the first and second quarters of 2021 (Figure 7)[60].
- Clients previously covered by one large policy now have to seek a panel of insurers, each covering only a 30-50% share of the 2020 coverage[61].

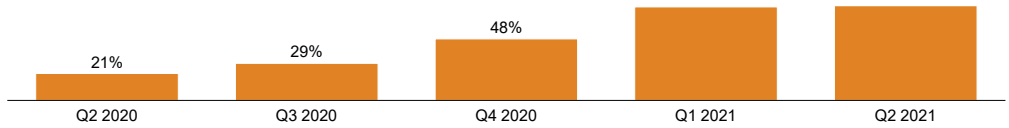
56 US cyber market update, Aon, June 2021
57 Loss ratio + expense ratio
58 US cyber market update, Aon, June 2020
59 US cyber market update, Aon, June 2021
60 Commercial Property/Casualty Market Index, The Council of Insurance Agents & Brokers, USA, 2021
61 John Farley, "2022 Cyber Insurance Market Conditions Report", Gallagher, January 2022

- Insurers are explicitly excluding cyber coverage from traditional policies to reduce the risk of "silent cyber", ie, cyber losses from traditional property and liability policies where cyber coverage is neither specifically included nor excluded, as these policies were often designed before cyber risks became apparent[62]. As cyber incidents often impact several of the insurers' lines of business, including property, business interruption, kidnapping and ransom risk, they can be the largest share of insurance losses if they are not explicitly excluded from the policy. For example, the total insured losses resulting from the Petya and NotPetya malware could be almost 90% attributed to silent cyber[63]. Cyber risk is now covered by insurers in a more transparent way via dedicated and innovative products specifically designed for this purpose.

Cyber risk now covered by dedicated insurance products

Figure 7: Cyber insurance capacities of carriers are being constrained

Global respondents reporting a decrease in cyber underwriting capacity — 2020−2021



Source: The Council of Insurance Agents & Brokers

In line with reviewing cyber-risk appetite, some insurers writing cyber business have also changed their underwriting criteria. The prerequisites for obtaining cyber insurance have become more advanced to reflect the increase in the number and type of losses. Insurers now conduct comprehensive risk and maturity reviews of their clients' cybersecurity readiness (eg, a lack of data-security controls can potentially result in a 100% to 300% increase in premiums or even no coverage at all)[64]. Furthermore, some underwriters do not offer cyber coverage for specific industries, including municipalities, higher education, technology and manufacturing[65].

Lack of data-security controls can increase premiums 100-300%

The 2021 USA cyber loss ratio results indicate that the policy changes worked from a profitability perspective. For US stand-alone policies, the loss ratio decreased from 73% in 2020 to 65% in 2021[66]. However, due to the associated increase in premiums needed to reach adequacy or to hardened underwriting criteria, some clients may no longer be able to afford coverage, resulting in an increased cyber protection gap.

Overall, the supply of cyber insurance has seen strong growth in the past five years. In terms of the coverage and services offered, cyber insurance policies are highly varied today and insurers have begun offering additional services beyond mere risk transfer, including *ex-ante* risk-mitigation services and the provision of post-breach resources, which have been identified as important factors besides risk transfer for clients looking for cyber insurance[67]. However, cyber is still an evolving market and the constantly developing risk exposures and often limited and inconsistent data present challenges for insurers. Although risk modelling has improved, it is still subject to high levels of uncertainty compared to other areas in which the data, products and pricing are highly advanced and mature, such as motor insurance. Moreover, the sharp increase in losses in 2020 made insurers cautious about their capacity allocation and operating model for

62 Bethan Moorcraft, "What is silent cyber risk?", Insurance Business America, 26 November 2018
63 "Making noise about 'silent' cyber", Allianz Global Corporate & Specialty, 2020
64 "Cyber market conditions", Gallagher, 2022
65 Ibid
66 "US cyber insurance sees rapid premium growth", Fitch, 2022
67 "Cyber insurance market watch survey", The Council of Insurance Agents & Brokers, 2016

cyber insurance. If losses stay at the same level of approximately 60-70% of GWP and if global cyber GWP continue to grow at 25-40%, total insured cyber risk exposure is expected to be US$13-25bn by 2025.

Economic impact of cyber incidents is at least US$1trn

There is no definitive figure for total cyber losses, as not all incidents are reported and quantified by businesses and national institutions. However, several research papers point toward estimates of more than US$1trn annually. The most widely used estimate from McAfee puts first-order losses at US$945bn annually (Figure 8)[68]. This estimate incorporates bodily injury, software and hardware replacement, cyber ransom payments and regulatory fines but excludes second-order losses, such as lost business or reputational damage. However, McAfee recognises that indirect losses (eg, losses due to interrupted business continuity) do also need to be considered[69].

Second-order losses (lost business and reputational damage) account for at least 60-70% of overall breach costs[70]. When adding these second-order losses to the MacAfee estimate, it approaches CyberSecurity Ventures' "all-in cost" estimate of more than US$6trn[71].

Figure 8: Cyber-incident loss estimates vary, but all show significant volumes

Global annual losses from cyber incidents — 2017−2020 ($trn)

Assessment of losses		Survey used	Included in calculation	Not included in calculation
Cybersecurity Ventures 2020	6	Unknown	All first- & second-order losses (incl. lost business, brand & reputational damage)[1]	—
McAfee 2020	0.95	1 500 IT & line of business decision-makers (USA, Canada, UK, Japan, Australia, France, Germany) extrapolated to a global number	Some of the first-order losses, which can be described as "monetary", eg, bodily injury, software & hardware replacement	System downtime, intellectual property theft, incident-response costs, legal & consulting costs, reduced efficiency, lost business & reputational damage
McAfee 2018	0.52			
Lloyd's 2017[1] (cites McAfee US$0.4-0.6trn 2014 estimate)	0.4	Published data, interviews & estimates by government agencies & global companies	All first- & second-order losses (incl. lost business, brand & reputational damage)	—
Cybersecurity Ventures 2015	3	Unknown	All first- & second-order losses (incl. lost business, brand & reputational damage)	—

1. *Cited in "Ten Key Questions on Cyber Risk and Cyber Risk Insurance", The Geneva Association, November 2016*

Sources: McAfee; Lloyd's; IBM; Cybersecurity Ventures

Number and cost of incidents push up losses 20% p.a.

All reports agree that losses seem to have been growing at approximately 20% per annum and that this growth rate could be higher in upcoming years due to even more advanced cyber attacks. Growth in estimated losses can be attributed to the increase in the number and cost per incident. The number of cyber incidents has been growing steadily since 2017. The average number of cyber attacks per company grew approximately 30% from 206 in 2020 to 270 in 2021, with the share of successful attacks likewise increasing (from 22% to 29%)[72]. Ransomware

68 "The hidden costs of cybercrime", McAfee, 2020
69 Ibid
70 Taking detailed calculations provided by IBM for data breach as an example in "IBM Cost of Data Breach Report 2021", IBM, 2021
71 Steve Morgan, "2017 Cybercrime Report", Cybersecurity Ventures, 2017
72 Kelly Bissell, Jacky Fox, Ryan LaSalle and Paolo Dal Cin, "State of cybersecurity resilience 2021 – How aligning security and the business creates cyber resilience", Accenture, 2021

frequency also increased in 2021, with SonicWall observing approximately 623 million ransomware attacks globally — a 105% increase on 2020 and a more than 300% increase on 2019[73].

The following trends influence the number of cyber attacks:

- **The commercialisation of and innovation in cyber attacks**. AI is now widely used by attackers to send phishing emails. Ransomware as a service (commercialising ransomware) and cryptocurrencies have significantly reduced the cost of conducting ransomware attacks and made them more widespread. At the same time, innovation is also used to prevent and secure a faster resolution from attacks. Organisations with fully deployed security AI and automation seem to be more protected from breaches, since AI and automation help reduce the time required to identify and contain them. These organisations' average data-breach costs are approximately US$2.9m, compared to around US$6.7m for organisations without security AI and automation[74]. As the share of organisations with fully or partially deployed security AI and automation is rising (65% in 2021 versus 59% in 2020)[75], this could indicate a trend towards more resilience.

- **The Internet of Things (IoT)**. As more "things" come alive with the power of digitalisation and internet protocols, so do new vulnerabilities and risks. While many of these issues only affect industrial organisations, any organisation that uses the IoT in its infrastructure is also increasingly exposed to risk. The use of industrial control systems or operational technology hardware increases vulnerabilities every year.

- **Remote working**. Remote working has increased the number of cyber incidents and costs. Specifically, the number of ransomware attacks spiked globally during the first wave of the COVID-19 pandemic in February and March 2020, with an increase of 148%[76]. Similarly, where remote work was a factor in causing the breach, the average total costs of data breaches were approximately US$1m higher than when remote work was not a factor[77]. For 18% of organisations, remote work was a factor in the data breach, and organisations with more than half of their employees working remotely took almost two months longer to identify and contain breaches than those with fewer working remotely[78].

Ransomware attacks spiked 148% in first wave of COVID-19

- **Political instability**. Global instability tends to trigger spikes in cyber attacks. For example, in 2020, Beijing-linked hackers hacked the Vatican's computer networks on the eve of negotiations between China and the Vatican[79].

Besides the number of cyberattacks, the costs per incident have increased in six of the last seven years, with a significant uptick in 2021. For example, the cost of a data breach increased by approximately 10% from 2020 to 2021 — the largest single-year cost increase in the last seven years (from US$3.86m in 2020 to US$4.24m in 2021)[80]. The cost of ransomware has also reportedly increased — from an average of approximately US$115 000 in 2019 to around US$570 000 in 2021[81].

73 "2022 SonicWall Cyber Threat Report", SonicWall, 2022
74 "Cost of a Data Breach Report 2021", IBM
75 Ibid
76 "Cybersecurity trends: Looking over the horizon", McKinsey, 10 March 2022
77 "Cost of a Data Breach Report 2021", IBM
78 Ibid
79 Cate Cadell, "US cybersecurity firm says Beijing-linked hackers target Vatican ahead of talks", Reuters, 29 July 2020
80 "Cost of a Data Breach Report 2021", IBM
81 Ramarcus Baylor, Jeremy Brown and John Martineau, "Extortion payments hit new records as ransomware crisis intensifies", Palo Alto Networks, 9 August 2021

Mega-breaches are a rising trend

Mega-breaches are a rising trend — with tech giants such as LinkedIn, Facebook and Alibaba targeted in 2020 and 2021 and 0.3 billion to 1.1 billion customer records being breached. The increased costs are expected to be primarily driven by two factors: firstly extortion demands and secondly compliance with national/local privacy laws is becoming more costly. According to DLA Piper, the EU issued US$1.2bn in fines related to cyber incidents in 2021 — a seven-fold increase on 2020[82].

Current cyber protection gap is more than US$0.9trn

Whereas first-order cyber losses are close to US$0.95trn annually[83], supply covers only approximately US$6bn. This leads to an estimated cyber protection gap of more than US$0.9trn between losses and what is covered today. While the cyber insurance gap will persist in the future, the overall share of uninsured losses will potentially decrease due to higher growth in insurance supply.

Businesses increasingly invest in cybersecurity

The question remains how businesses, insurers and governments can move towards reducing this emerging and growing frontier of risks. Businesses are already trying to "self-insure" against its rise. Since 2013, the cybersecurity market has grown much faster than the overall IT market[84] with more than 10% growth annually and close to US$160bn in revenue in 2022[85]. Businesses are investing in cybersecurity roadmap development and business continuity and are hiring digital forensics organisations as contractors to ensure faster incident resolution. However, these efforts may not be sufficient against the backdrop of rising cyber-attack innovations and geopolitical instability.

In addition, concerns about systemic cyber risk are rising. While the concept of systemic risk is rather vague, it can be described as "the risk or probability of breakdowns in an entire system, as opposed to breakdowns in individual parts or components"[86]. As digitalisation, interconnectedness and cloud services have increased rapidly, cyber risk can potentially become a systemic risk impacting multiple organisations or even nations. For example, the 2020 SolarWinds cyber incident showed how quickly cyber incidents can affect hundreds of organisations[87].

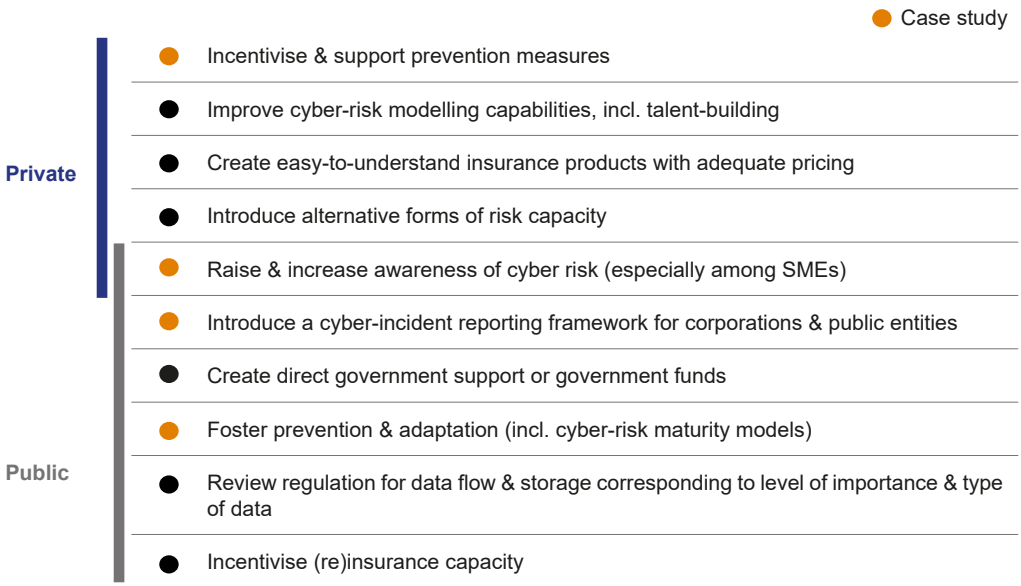
Due to the lack of diversification in the inherent nature of some risks, insurers have started — and are likely to continue — to exclude some risks from their policies. For example, insurers are acting to address one key cause of cyber risk: war-related activities. Munich Re refined its cyber insurance policies in April 2022 to exclude cyber war[88] and Lloyd's requires catastrophic state-backed attack exclusions in all stand-alone cyber-attack policies[89]. Hence, parts of the gap that are systemic by nature (ie, losses from entire system breakdowns) may not be addressed by insurers alone. The increasing frequency, severity and number of different types of cyber attacks and their potential systemic risk requires both public and private stakeholders to assess what role they should play in this fast-moving field and collaborate to sustainably manage the extreme tail risk.

82 Ross McKean, Ewa Kurowska-Tober and Heidi Waem, "DLA Piper GDPR fines and data breach survey: January 2022", DLA Piper, 18 January 2022
83 James Andrew Lewis, Zhanna Malekos Smith and Eugenia Lostri, "The hidden costs of cybercrime", McAfee, 9 December 2020
84 "Gartner forecasts worldwide IT spending to grow 3% in 2022", Gartner, 14 July 2022 and "Gartner says worldwide IT spending is forecast to be flat in 2016", Gartner, 7 July 2016
85 "Cybersecurity revenues, 2016–26", Statista
86 George Kaufman and Kenneth Scott, "What is systemic risk, and do bank regulators retard or contribute to it?", The Independent Review, 2003, Volume 7, Issue 3
87 US White House press briefing by press secretary Jen Psaki and deputy national security advisor for cyber and emerging technology Anne Neuberger, 17 February 2021
88 Carolyn Cohn and Noor Zainab Hussain, "Munich Re tightens up cyber insurance policies to exclude war", Reuters, 8 April 2022
89 Tony Chaudhry, "State backed cyber-attack exclusions", Lloyd's Market Association Bulletin, 16 August 2022

Variety of levers for public and private stakeholders

To close the cyber protection gap, a toolbox of potential levers that private and public stakeholders can use was identified (Figure 9). It is worth noting that the portfolio of levers chosen is expected to be highly specific to individual countries and will depend, for example, on the position of the insurance industry, past initiatives, the regulatory environment and certain policy choices. This toolbox of potential levers should not be considered as a list of recommendations but as a "menu" of possible actions.

Figure 9: Cyber protection gap — toolbox of potential levers



(For GFIA's cyber protection gap reduction recommendations, see the Executive Summary, p15.)

We have looked at various case studies (Figure 10) that illustrate how some of these levers have been put into practice in some parts of the world by private or public stakeholders.

Figure 10: Overview of case studies

	Levers	Case studies	Outcomes
Private	Incentivise & support prevention measures	Overarching: Cyber-risk engineering as part of insurers' product portfolios Financial incentives for prevention via policy clauses	**70%** Cyber-risk reduction through training
Public	Raise & increase awareness of cyber risk (especially among SMEs)	Government information campaign via TV, social media, newspaper & radio Annual cyber awareness poll & campaign for SMEs	**~2 mn** people reached with campaign **Increased media attention** on cyber threats
	Introduce a cyber-incident reporting framework for corporations & public entities	Cyber Incident Reporting for Critical Infrastructure Act in 2022 Security of Critical Infrastructure Act 2018 and expansion in 2021 to broaden scope of critical infrastructure Network & Information Security (NIS) Directive and General Data Protection Regulation (GDPR), requiring obligatory incident reporting for specific sectors	**Higher level of transparency**[1] on cyber incidents, enabling risk modelling
	Foster prevention & adaptation (incl. cyber-risk maturity models)	Cyber Defence Unit with voluntary members to ensure advanced IT skills against cyber attacks Cyber requirements defined as part of the EU Basel III and Solvency II regimes	**#3** most cyber-secure country in the world **Enhanced cyber security** enforced by regulatory framework

1. Quantitative impact estimate not yet available

Case studies

Prevention measures can eliminate 80-90% of cyber-incident costs

Incentivise and support prevention measures

According to the Ponemon Institute, prevention measures can potentially eliminate 80-90% of the costs of cyber incidents[90]. These measures aim to address human errors — the main contributing factor in approximately 95% of all cyber incidents[91] — and IT system shortcomings. Insurers incentivise prevention by providing value-added, *ex-ante* cybersecurity services and financial incentives through policy clauses. Value-added, *ex-ante* services include cyber-risk-engineering services, where insurers work closely together with their clients to identify potential improvements in their security standards (eg, password defence, phishing simulation, network vulnerability scanning and security benchmarking) and services to develop infrastructure together with the client in a secure environment. Financial incentives through policy clauses require organisations to demonstrate specific security standards to receive favourable insurance terms or even be eligible for coverage. In the following, both approaches to incentivising prevention measures are highlighted based on case studies.

A Swiss Re survey[92] found that approximately 70% of cyber insurance providers already offer or plan to offer additional value-added prevention services to their clients. Whereas some insurers provide these services through extensive in-house risk-engineering expertise, most insurers cooperate with external advisors such as cybersecurity providers[93].

90 "The economic value of prevention in the cybersecurity lifecycle", Ponemon Institute, USA, April 2020
91 IBM Security Services 2014 Cyber Security Intelligence Index, IBM, May 2014
92 "Cyber: In search of resilience in an interconnected world", Swiss Re, 1 October 2016
93 Ibid

Chubb is an example of an insurer that has developed an extensive network of in-house expertise in risk engineering. With over 400 risk-engineering professionals, Chubb provides risk-engineering services to its customers based on three pillars: risk assessment, risk management and risk partnership[94]. It offers a range of services, including a risk assessment of existing IT infrastructure, potential loss calculations in scenario-based analyses and tailored recommendations to build a more secure infrastructure for webinars and training for employees.

Zurich Insurance Group provides *ex-ante* risk-mitigation services through its partnership with CYE, an Israel-based cybersecurity provider, combining advanced AI with an extensive global network of more than 945 experts[95]. These services include a free, technology-based risk assessment and discounted prices for CYE's other services, such as simulations of cyber incidents.

Risk training can reduce cyber risks by up to 70%

Research shows that risk training can potentially decrease cyber risks by up to 70%[96]. Moreover, data from other insurance areas shows that preventive behaviour might be positively reflected in reduced insurance premiums, thus indicating that insurers consider such behaviour effective. For example, in the auto insurance sector, driver safety training can lower insurance premiums by approximately 5%, and pay-as-you-drive insurance potentially decreases insurance premiums by 10-20%. Additionally, a survey by Swiss Re found that 33% of companies already see these additional services as adding value[97]. Another survey identified them as one of the top three factors in purchasing cyber insurance among large companies[98]. While insurers certainly have incentives that are aligned with their clients' interests to mitigate cyber risk, as they otherwise carry the costs, they need to identify a suitable strategy for providing this expertise. This can be done by intensively recruiting skilled professionals to build their capabilities in-house, by acquiring an existing cybersecurity provider or through partnerships with third-party cybersecurity experts.

Besides offering *ex-ante* services and cyber coverage, some insurers also financially incentivise prevention through specific policy clauses. For example, HDI Germany includes an awareness clause in its cyber policies that reduces the deductible by 25% if the policyholder uses HDI's free prevention services that are offered alongside the coverage. Additionally, policyholders can further reduce their deductible by 75% if they conduct a "baseline security check" through HDI's subsidiary Perseus, an IT security service provider[99].

Similarly, insurers including Allianz, Munich Re and Beazley offer favourable coverage conditions through participation in the "Cyber Catalyst by Marsh" programme. This programme aims to create transparency in the cybersecurity market by bringing together insurers' expertise to evaluate existing cybersecurity products. Organisations adopting products certified by the Cyber Catalyst may receive enhanced coverage from their insurer. While these policies motivate organisations to consider investing in prevention, they might incentivise companies to only invest in security measures when applying for their cyber insurance coverage. Thus, insurers must continuously ensure adherence to security standards and incentivise prevention measures for the entire duration of insurance coverage.

In addition to *ex-ante* services and financial incentives in policy clauses, some insurers have

94 "Cyber risk engineering", Chubb, 2021
95 "Zurich Cyber Security Services", Zurich, 2022
96 Georgios Pouraimis et al., "Long lasting effects of awareness training methods on reducing overall cyber security risk", Defense & Commercial Sensing, 7 May 2019
97 "Cyber: In search of resilience in an interconnected world", Swiss Re, 1 October 2016
98 "Cyber Insurance Market Watch Survey", The Council of Insurance Agents & Brokers, 2016
99 "HDI Cyberversicherung für Firmen und Freie Berufe", HDI

expanded their offerings to provide post-event rectification services. For example, Beazley has built a separate business unit, Beazley Breach Response Services, to support its clients in handling cyber incidents. The services provided cover forensic investigations into the scope of the cyber incident, legal responsibility assessments, PR handling and notifying affected individuals. Similarly, Allianz Global Corporate & Specialty offers its clients incident-response services to provide 24/7 access to legal and IT experts, as well as crisis and communication support.

These examples highlight how insurers expand their client offerings to include risk management solutions, *ex-ante* preventive and *ex-post* incident-response services. By incentivising prevention to build cyber resilience in their clients' organisations, insurers can potentially address the cyber protection gap. As research has found, preventive efforts can potentially reduce the likelihood and costs of cyber attacks, thereby increasing insurability, and insurers can foster these by leveraging their capabilities in risk assessment. However, insurers can only support prevention; organisations need to be aware of their exposure to and responsibility for cyber risks.

Raise and increase awareness of cyber risk (especially among SMEs)

Overall, a lack of cyber-risk awareness may increase individual behaviour that puts organisations at risk, such as connecting to public Wi-Fi networks or downloading unauthorised applications[100], and hold back preventive measures and cyber insurance if organisations are unaware of the potential costs. According to the EU Agency for Cybersecurity (ENISA), 84% of cyber attacks rely on social engineering (ie, phishing)[101].

SMEs can be particularly vulnerable to cyber attacks

SMEs may be particularly vulnerable to cyber attacks as they invest fewer resources in security while still handling sensitive information such as personnel and customer information, financial data or production details. As digitalisation is increasing rapidly among SMEs, most recently driven by the COVID-19 pandemic, information-security literacy and implementation may not always be able to keep up[102]. In a 2021 US SME survey, over 50% of SMEs indicated that cyber risk does not apply to them[103]. Some even showed an "it will never happen to me" mentality and may, therefore, not invest in effective prevention and defence measures[104,105]. Stakeholders, including public and private players, could address this proactively by educating the public, especially SMEs, on cyber threats and cyber-insurance options and their importance.

- Sweden is one country where awareness initiatives are potentially addressing parts of the cyber protection gap. The 2018 Swedish national strategy for information- and cybersecurity recognised the need for increased awareness. The Swedish Civil Contingencies Agency was tasked with a national information campaign to increase knowledge about information security and identity theft[106]. The campaign specifically focused on increasing awareness of the need to protect one's most valuable information to incentivise behavioural change. To achieve this, the Agency worked with external partners and other government authorities to produce information in the form of films, banners, messages and a campaign website. For SMEs, it included new guidance on technical security actions and routines, partner activities

100 Anna Sarri and Radu Arcus (eds.), "Raising awareness of cybersecurity: A key element of national security strategies", ENISA, 29 November 2021
101 Anna Sarri, Viktor Paggio, and Georgia Bafoutsou (eds.), "Cybersecurity for SMEs: Challenges and recommendations", ENISA, 1 June 2021
102 Ibid
103 Ho-Tay Ma, Christopher McEvoy and Andrew Laing, "Cyber insurance – The market's view", PartnerRe, 17 September 2020
104 Ibid
105 Isabel Lopes and Pedro Oliviera, "Applying Action Research in the Formulation of Information Security Policies", 2015
106 Marianne Björkman, "Att stärka allmänhetens samt små och medelstora företags motståndskraft mot it-incidenter", Myndigheten för samhällsskydd och beredskap, 14 January 2019

such as seminars, tests and events, and a new IT security standard that was developed with the Swedish Theft Prevention Association and industry partners. The campaign reached 50% of the target audience (25- to 45-year-olds, who are most likely to be affected by fraud), exceeding its 41% goal. In absolute numbers, 750 000 visitors were exposed to the films via SF Studios cinemas, 1.9 million via Tv4 (a popular TV channel), and 1.1 million via social media[107].

- Another example of a public awareness campaign comes from a national industry association in Canada. The Insurance Bureau of Canada (IBC) also focused its attention on increasing cybersecurity awareness in SMEs after a poll it commissioned in 2019 showed a significant lack of awareness and protection among them[108]. In the survey, 44% of SMEs with fewer than 500 employees indicated that they had no defences against cyber attacks and 60% had no cyber insurance. SMEs contributed 51.9% to Canada's private-sector GDP in 2018 and 79.4% to private-sector employment[109], yet, according to the Canadian Federation of Independent Business, 60% of small businesses go bankrupt within six months of suffering a cyber attack, making this a significant economic concern[110].

60% of Canadian small businesses go bankrupt within 6 months of attack

  To address this problem, the IBC published a series of infographics, videos and social media communications to inform SMEs about cyber risk and cybersecurity measures. In 2020, it published additional resources related to the COVID-19 pandemic's impact on cybersecurity[111]. The campaign is still running and the IBC will continue to track its reach. Already, there has been an increase in the cybersecurity market in Canada. In 2019, GWP for cyber insurance were approximately C$135m (US$100m) and they increased to approximately C$222m in 2020[112]. While no causality between the awareness campaign and the rise in premiums can be proved, the campaign was most likely to have been a contributing factor to the increase in awareness.

  In addition, IBC launched in 2022 the "Cyber Savvy" campaign, polling employees at SMEs on cybersecurity. The survey found that 42% of respondents had seen an increase in scam attempts over the last year. However, only 34% reported that their employers were providing mandatory cybersecurity-awareness training. Also, 72% of respondents reported at least one behaviour that could allow a cybercriminal to access their organisation's computer systems (such as sharing passwords or unauthorised downloading of software).

Worldwide cyber-risk awareness is rising

Globally, the number of cybersecurity awareness campaigns and overall awareness of cyber risks is increasing. For example, the German Insurance Association (GDV) offers an online risk assessment tool for SMEs that includes specific recommendations to improve security[113], the General Insurance Association of Korea offers educational projects (discussions, seminars and leaflets)[114] and the USA Cybersecurity and Infrastructure Security Agency runs a national public awareness campaign[115]. The French Insurance Association, France Assureurs, has published a digital-risk awareness kit for assessing, anticipating and minimising cyber risk[116]. And GFIA has

107 Ibid
108 "Towards a safer cybersecurity environment: Insurance industry cyber-awareness initiatives", GFIA, January 2021
109 "Key Small Business Statistics — 2021", Innovation, Science and Economic Development Canada
110 "Facts about cyber crime", Insurance Bureau of Canada, 9 October 2018
111 "Towards a safer cybersecurity environment", GFIA, January 2021
112 Bethan Moorcraft, "Cyber security needs to be 'democratized' for small businesses", Insurance Business Canada, 15 October 2021
113 Christian Siemens and Melina Maier (eds.), "Cyberrisiken im Mittelstand 2020", GDV, 2020
114 "Towards a safer cybersecurity environment 2021", GFIA, January 2021
115 "About the CISA cybersecurity awareness program", US Cybersecurity and Infrastructure Security Agency
116 "Anticiper et minimiser l'impact d'un cyber risque sur votre entreprise 2021", France Assureurs, 15 January 2021

published a report giving an overview of cyber-awareness campaigns by various insurance industry associations worldwide to foster learning from successful initiatives[117].

While causality is hard to measure, this increase in awareness campaigns is likely to be one factor contributing to the overall increase in cybersecurity awareness, another one being the increase in the frequency and severity of attacks. Munich Re's "Global Cyber Risk and Insurance Survey 2022" measured an increase in respondents who are "extremely concerned" about a potential cyber attack on their company from 30% to 38% within a year[118]. The number of companies that are aware of cyber insurance is also increasing. In Germany, the percentage of medium-sized companies that took up cyber insurance in 2022 (44%) was double that in 2018, while the percentage that did not know about cyber insurance fell from 37% to 22%[119].

In summary, the case studies show a large amount of effort from the public and private sectors to increase cyber-risk and cybersecurity awareness. To reliably assess the impact of such campaigns, more empirical evidence is required, such as by defining impact KPIs ahead of the implementation of awareness campaigns and continuously monitoring them. Global developments in cybersecurity awareness and the growth of the cybersecurity market suggest the effectiveness of awareness campaigns and, consequently, their potential as a tool to address the cybersecurity gap by improving general cybersecurity behaviours, increasing cyber resilience and rendering access to insurance easier.

Introduce a cyber-incident reporting framework for corporations and public entities

Incident reporting remains low

According to US Senator Mark Warner, only 30% of US cyber incidents are currently being reported[120], leaving the majority of incidents undetected by public authorities. Estimates from the Crime Survey for England and Wales even indicate that the number of reported cyber incidents is below 2%[121]. As a result, governments, security agencies and insurers face challenges estimating the frequencies, magnitudes and probabilities associated with cyber incidents. Consequently, the market for cyber insurance is relatively small, as insurers cannot make reliable loss predictions and perform consistent and risk-adequate pricing. To gain transparency over cyber threats and effectively mitigate risks, governments across the world are starting to introduce regulations that enforce standardised incident reporting, such as the three described below.

- In the USA, laws obliging the notification of cyber incidents have been implemented at state level for around 20 years. The California Senate Bill 1386 — the first cyber-incident reporting law — was enacted in 2002 and became effective in 2003. Under the law, companies are required to notify any Californian resident whose data has been compromised in a data breach. Furthermore, the law obliges organisations to report larger breaches that affect more than 500 individuals to the attorney general[122].

  Following California, multiple states introduced similar legislation shortly afterwards and today all US states have cyber-incident reporting laws in place[123]. An Aon analysis demonstrates that the number of cyber incidents reported in the USA strongly correlates

117 "Towards a safer cybersecurity environment", GFIA, January 2021
118 "Munich Re Global Cyber Risk and Insurance Survey 2022", Munich Re, 1 August 2022
119 "Im Mittelstand steigt das Interesse an Cyberversicherungen", GDV, 19 July 2022
120 "Cyber in the Ukraine invasion", US Center for Strategic & International Studies, 14 March 2022
121 Nick Stripe, "Crime in England and Wales: year ending September 2020", UK Office for National Statistics, 3 February 2021
122 Data security breach reporting, US State of California Department of Justice, Office of the Attorney General, 2022
123 "Cyber incident reporting requirements & notification timelines for financial institutions", Bank Policy Institute, USA, 30 April 2022

with the growth in its cyber insurance market, thus indicating that such legislation has the potential to address the cyber protection gap[124].

Number of US incidents strongly correlates with insurance market growth

Following the 2020 SolarWinds hack — one of the largest cyber attacks that affected at least 100 private-sector companies and nine federal agencies[125] — in 2022 the USA introduced the Cyber Incident Reporting for Critical Infrastructure Act as the first federal cyber-incident reporting law. The new law will require critical-infrastructure companies to report any substantial cybersecurity incidents or ransom payments to the Cybersecurity and Infrastructure Security Agency within 72 and 24 hours respectively[126]. In total, 16 sectors currently fall under the Agency's definition of critical infrastructure, including the chemical, communications and financial services sectors. While the Act was signed in 2022, the Agency has until 2025 to publish the final rules. In the meantime, it encourages companies to share their incident data voluntarily and aims to publish it anonymously in a report to help other organisations manage their risk. Additionally, in March 2022, the US Securities and Exchange Commission proposed a new regulation that — if enforced — would oblige all publicly-listed companies to report any cyber incidents[127]. These new regulations are intended to provide more transparency than state-level legislation.

- In Australia, the first regulation covering standardised cyber-incident reporting was established with the Security of Critical Infrastructure Act 2018 (SOCI Act). The original regulation covered four sectors: water, electricity, gas and ports[128] but it was extended in 2021 to broaden the definition of critical infrastructure to 11 sectors, including financial services, transportation and communications[129]. Similarly to the Cyber Incident Reporting for Critical Infrastructure Act in the USA, the SOCI Act requires critical infrastructure companies to report any significant or relevant incidents to the Australian Cyber Security Centre within 12 and 72 hours respectively[130]. The Centre has also published a template on its website, which simplifies the reporting process for organisations and facilitates the standardisation of incident data[131]. Since 2020, the Centre has published collected incident data in an annual report highlighting trends, statistics and strategic assessments of cyber threats.

- In the EU, the Network and Information Security (NIS) Directive came into force in 2018. This first EU-wide cybersecurity regulation aims to harmonise the cybersecurity regulation for critical sectors, as member states previously had different levels of regulation in place. The NIS Directive introduced cyber-incident reporting rules for digital service providers and operators of essential services, including energy, transportation, finance and health, which member states were required to incorporate into national law. It further required member states to set up dedicated Computer Security Incident Response Teams, to which major cyber incidents should be reported[132]. In addition to the NIS Directive, the EU General Data Protection Regulation, which also came into force in 2018, includes an obligation for every

124 "Global Cyber Market Overview: Uncovering the Hidden Opportunities", Aon Inpoint, June 2017
125 US White House press briefing by press secretary Jen Psaki and deputy national security advisor for cyber and emerging technology Anne Neuberger, 17 February 2021
126 "Cyber Incident Reporting for Critical Infrastructure Act of 2022", Cybersecurity and Infrastructure Security Agency, 2022
127 "SEC proposes rules on cybersecurity risk management, strategy, governance, and incident disclosure by public companies", US Securities and Exchange Commission, 9 March 2022
128 "Security of Critical Infrastructure Act 2018", Australian Government, 2018
129 "Security of Critical Infrastructure Act 2018", Australian Government, 2021
130 Ibid
131 "Report a cyber security incident", Australian Cyber Security Centre, 2022
132 Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, Article 1

organisation to notify the relevant data protection authority of any incident involving personal data breaches within 72 hours[133].

Insurers need incident data to develop and price products

To adequately address the protection gap, it is crucial that the information on cyber incidents is shared with insurers (in an aggregated and anonymised format) to enable the provision of adequate products and pricing. Some countries have started to publicly share anonymous data on cyber incidents. For example, the US National Association of Insurance Commissioners (NAIC) has been collecting cyber-incident data from insurers annually through the Cybersecurity and Identify Theft Supplement of its Property/Casualty Annual Statement since 2016. These findings and alien surplus lines data collected through the NAIC's International Insurers Department are published in an annual report, together with an analysis of developments in the cyber insurance market. In 2022, 152 insurance groups submitted data to the cyber supplement[134].

To summarise, public players are taking an active role in cybersecurity by introducing regulations aimed at increasing cybersecurity, helping to understand cyber threats and developments, and, to a lesser extent, providing more market transparency. Recently introduced national legislation might have the potential to increase transparency over the probabilities, types and economic costs of cyber incidents. However, as these regulations have only been introduced recently and some will only be enforced in the coming years, their actual impact is still to be assessed. Moreover, governments and public authorities need to find ways to securely share data with insurers to address the cyber protection gap effectively.

Foster prevention and adaptation (including enacting cyber risk maturity models)

Governments worldwide have put cybersecurity on their national agenda, introduced cybersecurity strategies with clearly defined national cybersecurity objectives and set up related public support initiatives to build national cyber resilience and educate people about safe data usage and storage. The efforts include prevention and adaptation measures.

- On 27 April 2007, Estonia was hit by a severe cyber attack that was part of a larger conflict resulting from a public disagreement over relocating a Soviet-era bronze statue of a soldier from the centre of Tallinn to the city's outskirts[135]. The cyber attack lasted 22 days[136], took down multiple banks, news agencies and public authorities, and was the first cyber attack on an entire nation[137].

  Following the attack, Ülo Jaaksoo, an Estonian computer scientist and CEO of a leading Estonian R&D and manufacturing software solutions company, proposed the introduction of a Cyber Defence League[138]. At around the same time (May 2008), the Estonian government's Cyber Security Strategy also highlighted the importance of public-private sector cooperation to build cyber resilience[139]. As a result, the Estonian Cyber Defence Unit was officially established in January 2011 as a sub-unit of the existing Estonian Defence League. The unit is based on active voluntary membership, for which Estonian citizens can apply if they fulfil a set of requirements, including knowledge of information security, and it aims "to protect

133 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, Article 33
134 "Report on the Cyber Insurance Market", National Association of Insurance Commissioners, USA, 18 October 2022
135 Damien McGuinness, "How a cyber attack transformed Estonia", BBC News, 27 April 2017
136 Rain Ottis, "Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective", NATO Cooperative Cyber Defence Centre of Excellence, 2008
137 Damien McGuinness, "How a cyber attack transformed Estonia", BBC News, 27 April 2017
138 Anna-Maria Osula, Kadri Kaska and Jan Stinissen, "The cyber defence unit of the Estonian Defence League", NATO Cooperative Cyber Defence Centre of Excellence, 2013
139 "Cyber security strategy", Republic of Estonia Ministry of Defence, 8 May 2008

Estonia's high-tech way of life by protecting information infrastructure and supporting the broader objectives of national defence"[140].

The Estonian Cyber Defence Unit is built on three pillars. The first is focused on fostering cooperation among IT professionals and provides an expert network for information-sharing between private and public players. The second is concerned with the improvement of critical-infrastructure security, focusing on increasing awareness and sharing best practices on IT security and developing contingency plans for operating during crises. The third pillar concentrates on improving education and expertise by continuously providing training to all members. The Unit has been widely recognised as an innovative cybersecurity model. Estonia has entered into agreements with Austria, Luxembourg, Singapore, South Korea and NATO on sharing cyber expertise[141]. Moreover, in 2021 Estonia was recognised as the third-most cyber-secure country in the world and the most secure in Europe by the Global Cybersecurity Index[142].

While the case study from Estonia illustrates how a nation has built up its cyber resilience through a dedicated governmental unit focused on cybersecurity, other countries are fostering cyber resilience on a legislative level by introducing minimum security standards. Moreover, besides fostering prevention, several governments have also introduced adaptation measures that ensure risk mitigation in the event of an attack.

- To address gaps and fragmentation in cybersecurity regulation, the European Commission proposed the Digital Operational Resilience Act at the end of 2020. The Act[143] entered into force in January 2023 and aims to strengthen the IT security of EU financial institutions and harmonise digital operational resilience.

Other countries are also introducing forms of cyber-risk maturity models. For example, in 2021, the South African Financial Sector Conduct Authority and the Prudential Authority published a draft joint standard, "Cybersecurity and Cyber Resilience Requirements"[144]. The standard aims to define minimum standards for financial institutions to ensure cybersecurity and resilience practices.

Governments have variety of levers to foster prevention and adaptation

In summary, governments could implement regulations focusing explicitly on cyber risk *ex-ante* to ensure resilience and stability in the event of a cyber incident. Government support can take various formats to foster prevention and adaptation. These range from national cybersecurity strategies and preventive efforts to legislation on prevention and adaptation measures in the form of minimum standards based on a risk maturity model or required risk capital. Together, these efforts could effectively address the cyber protection gap by providing resources and a regulatory framework for the market.

Additional levers for private players

Below are additional levers that can be used by private players to address the cyber protection gap. They aim to build a basis for creating appropriate products through standardised incident-data collection and improved modelling capabilities.

140 "Estonian Defence League's Cyber Unit", Estonian Defence League, 2022
141 "Estonia and Singapore concluded a cyber cooperation agreement", Republic of Estonia Ministry of Defence, 18 January 2018
142 Global Cybersecurity Index, International Telecommunication Union, 2021
143 Regulation (EU) 2022/2554 on digital operation resilience for the financial sector
144 Mark Bechard, "Draft standard on cybersecurity published for comment", Moonstone, 6 January 2022

Create easy-to-understand insurance products with adequate pricing

Cyber insurance products will need to continue to evolve to match the risks that customers face. Currently, some cyber protections may be offered as part of P&C packages, while some need to be purchased separately. A prime example is insurance for state-sponsored or terrorist cyber incidents, which is excluded from packaged P&C offers and has to be purchased separately[145]. Coverage of cyber attacks causing physical damage could also further be explored. In addition, the pricing of these products might need adjusting to align with insurers' risk appetite and strategy.

While pricing could be fixed by providing more transparency over losses and incidents, clear affirmation or exclusions of cyber coverage could provide certainty for both the insurer and the insured and significantly increase penetration and combat "silent cyber" risks. Underwriters are working on several pricing aspects to enhance overall resilience: improved assessment of cyber-risk controls; improved pricing tools; clear statement of exclusions of cyber cover; management of systemic risk; development of new products that match customers' evolving needs; and development of risk-management solutions.

Improve cyber-risk modelling capabilities, including talent building

Modelling cyber risk is crucial for insurance products and pricing

As the frequency and variety of cyber incidents gain momentum, insurers must find sustainable ways to insure cyber risk. Modelling cyber risk becomes crucial to ensure the right products and pricing. Insurers investing in new solutions and building up talent to keep up with technological advancements could thus ensure a greater supply of more appropriate cyber coverage and address the protection gap.

Introduce alternative forms of risk capacity

Cyber insurance-linked securities (ILS), including cyber bonds — an equivalent to natcat bonds — could be an alternative to cyber insurance and pass the risk to a broader pool of investors[146]. While several forms have already been considered, better risk modelling is needed before these can become widely available. In addition, this lever's danger of causing moral hazard[147] should be assessed, as cyber incidents are human-made and could therefore be manipulated.

Additional levers for public players

In addition to private players' efforts, governments can use the following levers to enforce cybersecurity and reporting regulations:

Create direct government support or government funds

Government funds similar to natcat funds could be set up to manage the consequences of cyber incidents. Given the size of some recent cyber incidents, a discussion will be required on the types of incidents that would trigger the support of government funds. Overall, this could be used as a "last resort" for losses above a certain threshold or certain types of incidents.

Review regulation for data flow/storage

There are indications that regulations forcing data localisation within country or regional geographic boundaries make data less secure and more vulnerable to cyber attacks. For

145 "Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation", OECD, 2020

146 Nathan Bruschi, "Maybe Wall Street has the solution to stopping cyber attacks", Wired Magazine, 2 June 2016

147 Moral hazard is the lack of incentive for a person to guard against risk when they are protected from its consequences

example, such laws could curtail the ability of organisations to establish integrated cyber risk-management systems or outsource cybersecurity management to suitable service providers[148]. Yet many legislators and jurisdictions are reluctant to allow the free flow of data because they are concerned about the differing levels of data protection outside their borders[149]. While drafting data-localisation laws, legislators might need to consider cyber risks as an unintended consequence and review data-flow regulations corresponding to different data types and levels of importance for data security.

Incentivise (re)insurance capacity

Due to the potential systemic risk in cyber threats, insurers face challenges insuring all losses. Public-private partnerships could therefore help manage the extreme systemic tail risk inherent in cyber. Similar to natcat funds, cyber funds could increase the overall supply of cyber insurance and stabilise coverage prices. As cyber insurance matures, it is important for all stakeholders to collaborate to understand existing and emerging policies and what they cover. Governments could then take proactive steps by setting up pooling mechanisms for the systemic part of cyber risk, which insurance cannot cover.

Additional levers that some public players may consider — despite their potentially controversial nature — are the prohibition of ransomware payments, mandated cybersecurity coverage and reinforcement of law enforcement:

Prohibiting ransomware payments could have unintended consequences

- **Prohibit ransomware payments**, eg, for medium and large corporations. Since 2021, a number of legislative initiatives have been implemented to prohibit ransomware payments, starting with government entities[150]. However, such measures could have unintended consequences for private and public entities, and thus the risk-benefit balance of such a lever needs to be assessed. In an environment where many organisations do not have the capacity to defend themselves, not being able to pay a ransom could result in insolvency, given that they have no other options. And public entities could lose oversight and control of ransomware payments, as affected organisations could pay them without involving public entities. Alternatively, legislative bodies could remove the tax deductions for ransomware payments that currently exist in some US states[151].

- **Mandate cybersecurity coverage**, eg, for large corporations in crucial economic sectors. For example, South Korea requires all financial institutions to buy cyber-liability insurance policies[152]. Mandatory coverage is a possible measure that needs to be weighed against unintended consequences, ie, increased insurance coverage costs for SMEs and potentially less motivation to take preventive measures and incentivise good behaviour against cyber attacks, particularly if prices are not directly linked to each company's risk exposure, which also limits the ability of insurers to offer a diverse range of products.

- **Reinforce law enforcement** to increase the risk for cyber criminals and thus discourage some of them, despite potential barriers to implementation given the cross-border nature of cyber attacks and difficulties in attribution.

148 DeBrae Kennedy-Mayo and Peter Swire, "The effects of data localization on cybersecurity", Georgia Tech Scheller College of Business, Research Paper No. 4030905, 24 June 2022
149 Anupam Chander, "Is data localization a solution for Schrems II?", Journal of International Economic Law, September 2020
150 "Cybersecurity Legislation 2021", National Conference of State Legislatures, USA, 1 July 2021
151 Ciaran Martin and Tarah Wheeler, "Should ransomware payments be banned?", Brookings Tech Stream, 26 July 2021
152 "Towards a safer cybersecurity environment", GFIA, January 2021

The case studies provide examples of how private and public players in different regions address the cyber protection gap. The initiatives aim to incentivise and support cybersecurity measures to build resilience across organisations, increase awareness of cyber threats and insurance, mandate incident reporting for increased transparency over economic exposure, and foster prevention and adaptation through governmental support and regulatory frameworks. The highlighted case studies show that these levers have the potential to (at least partially) address the cyber protection gap. Given the current size of the gap, additional levers from the toolbox can be used depending on their suitability for a particular region, weighing their potential unintended consequences against their likely impact.

Concluding remarks

Post-pandemic remote working has increased cyber risk

The increase in digitisation and automation and the shift to remote working due to the COVID-19 pandemic have significantly increased cyber risk in recent years, while the market for cyber protection (including but not limited to insurance coverage) is still nascent, resulting in a protection gap of more than $0.9trn.

An increasing number of insurers are trying to find sustainable ways of ensuring cyber coverage in order to grow cyber coverage supply in the coming years. Firstly, insurers have been able to gather more data over the past few years and hence refine their approach to this risk. Pricing and underwriting are thus more accurate today than in the past. Also, more and more insurers are entering the cyber insurance market, which translates into an increase in the supply. Finally, clarity has been brought to coverage and exclusions. All of this has allowed insurers to propose a more robust answer to the increase in the frequency, severity and types of cyber incidents.

As the current supply covers less than 1% of cyber losses, it can be assumed that the cyber protection gap will most likely grow in absolute terms in the next few years, despite possibly decreasing in relative terms. Moreover, concerns about cyber incidents becoming a systemic risk challenge insurers to provide appropriate products. To address the cyber protection gap, public and private players must thus assess their roles and collaborate by using the levers that are most suitable for the individual country or region.

GFIA Global Protection Gap Report Taskforce

Olav Jones, GFIA secretariat

Hirofumi Kurata, GFIA secretariat

Members:

Suzanne Williams-Charles, Association of Bermuda Insurers and Reinsurers (ABIR)

Jonathan Purvis, Association of British Insurers (ABI)

Andrew Melnyk, American Council of Life Insurers (ACLI)

David Snyder, American Property Casualty Insurance Association (APCIA)

Susan Murray, Canadian Life & Health Insurance Association (CLHIA)

Alain Caplan, Corporation of Lloyd's

Emilie Bel, France Assureurs

Jordan Brennan, Insurance Bureau of Canada (IBC)

Nicolas Jeanmart, Insurance Europe

Helen Dalziel, International Underwriting Association of London (IUA)

Dennis Burke, Reinsurance Association of America (RAA)

Pamela Remagaga, South African Insurance Association (SAIA)

Brussels, March 2023

www.GFIAinsurance.org

@GFIAinsurance

Global Federation of Insurance Associations