Allianz

Allianz Global
Corporate & Specialty

Cyber: The changing threat landscape

Risk trends, responses and the outlook for insurance

About AGCS

Allianz Global Corporate & Specialty (AGCS) is a leading global corporate insurance carrier and a key business unit of Allianz Group. We provide risk consultancy, Property-Casualty insurance solutions and alternative risk transfer for a wide spectrum of commercial, corporate and specialty risks across nine dedicated lines of business and six regional hubs.

Our customers are as diverse as business can be, ranging from Fortune Global 500 companies to small businesses. Among them are not only the world's largest consumer brands, financial institutions, tech companies, and the global aviation and shipping industry, but also floating windfarms or Hollywood film productions. They all look to AGCS for smart solutions and global programs to their largest and most complex risks in a dynamic, multinational business environment and trust us to deliver an outstanding claims experience.

Worldwide, AGCS operates with its own teams in more than 30 countries and through the Allianz Group network and partners in over 200 countries and territories, employing around 4,250 people. As one of the largest Property-Casualty units of Allianz Group, we are backed by strong and stable financial ratings. In 2021, AGCS generated a total of €9.5bn gross premium globally.

www.agcs.allianz.com

Contents

Introduction

Given cyber crime incidents are now estimated to cost the world economy in excess of $1trn a year[1] –around 1% of global GDP – it is no surprise that cyber risk regularly ranks as a top customer concern in the **Allianz Risk Barometer**, our annual survey identifying the top business risks around the world (including finishing #1 in the 2022 edition). Indeed, AGCS' own insurance industry claims analysis shows that external attacks are responsible for more than 80% of the value of the 3,000 cyber-related claims we have been involved with over the past five years around the globe.

This report highlights some of the main cyber risk trends we see from an underwriting, risk consulting and claims perspective, such as the growing cost of ransomware attacks – which has been the major loss driver in recent years, the targeting of more smaller-sized companies by hackers, the increasing frequency and sophistication of business email compromise attacks in the 'deep fake' era, as well as the impact of wider geopolitical tensions.

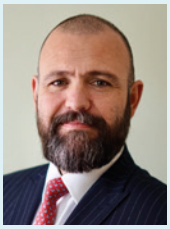
Our analysis shows that business interruption is the main cost driver in more than 50% of all cyber claims we participate in, and the report also highlights some of the major exposures that can result in large loss activity for companies. Of course, almost any cyber incident can also lead to litigation or demands for compensation from affected customers, suppliers and data breach victims, and elsewhere we look at the continuing evolution of third-party liability exposures, and how cyber security is increasingly seen as an environmental, social, and governance (ESG) issue. We also examine how a talent shortage is hindering efforts to improve cyber security.

In response to the challenging loss environment of recent years, the insurance industry is more diligently assessing clients' cyber risk profiles and clarifying coverage areas in a bid to incentivize companies to improve cyber security and risk management controls.

Our experience shows a number of companies still need to improve their frequency of IT security training, cyber incident response plans and cyber security governance. Incident response is critical as the cost of a claim quickly escalates once business interruption kicks in.

It is clear that organizations with good cyber maturity are better equipped to deal with incidents. It is not typical for us to see companies with strong cyber maturity and security mechanisms suffer a high frequency of 'successful' attacks. Even where they are attacked, losses are usually less severe.

The good news is that we are now seeing a very different conversation on the quality of cyber risk than we were a few years ago and are therefore gaining much better insights as the cyber insurance market matures. Insurers have a role that goes beyond pure risk transfer, helping clients adapt to the changing risk landscape and raising their protection levels. The more we can partner with our clients the more losses will hopefully reduce in future.



Scott Sayce
Global Head of Cyber and Group Head of the Cyber Centre of Competence
AGCS

1 McAfee and Center for Strategic and International Studies (CSIS), The Hidden Costs of Cyber Crime

Threats

Ransomware threat continues to help drive elevated cyber claims activity

In recent years AGCS has experienced elevated levels of cyber insurance claims, driven in part by the growth of the cyber insurance market, but also by an overall rise in incidents, including notifications of ransomware attacks, which are among the biggest drivers of cyber insurance losses. During 2020 and 2021, AGCS received more than 1,000 cyber-related claims per year overall and while claims activity has stabilized, driven by a more diligent underwriting approach and better risk dialogue with companies, 2022 has the potential to be another year of high claims frequency, as cyber claims historically have occurred predominantly in the third and fourth quarters of the year.

Despite the efforts of law enforcement agencies, the frequency of ransomware attacks remains high, as does related claims activity. Ransomware attacks hit a record 623 million[2] in 2021, double the number in 2020 and a 232% increase since 2019. Despite a 23% reduction in frequency at the start of this year, the number of ransomware attacks globally in the first half of 2022 still exceeded full-year totals of 2017, 2018 and 2019, according to SonicWall's Cyber Threat Report[3], while Europe actually recorded a 63% surge in ransomware attacks in the first half of 2022. Meanwhile, ransomware is forecast to cause $30bn in damages to global organizations by 2023, remaining the top cyber threat to enterprises as well as governments, according to cyber protection industry estimates[4].

There is no denying that cyber extortion, and ransomware, has become big business. Ransomware-as-a-service (RaaS), which gives cyber criminals access to ransomware tools and support services, has lowered the barriers to entry and enabled criminals to scale up their efforts and ramp up their attacks. With average ransom demands in 2021 in the millions and RaaS kits costing as little as $40 per month, cyber criminals can make huge returns with little investment or technical expertise from ransomware attacks.

On a positive note, there are some signs, however, that risk management actions taken by insured companies are beginning to take effect *(see section: The cyber risk management partnership)* and the AGCS ransomware protection checklist), yet overall the frequency and severity of ransomware and cyber extortion claims for AGCS has increased significantly in recent years.

"The number of ransomware attacks overall remains high," says **Rishi Baviskar, Global Cyber Experts Leader, Risk Consulting, AGCS.** "It is not possible to stop every cyber-attack and there are still a large number of companies that need to improve their defenses. Awareness is increasing and there have been improvements in cyber security, but more than half of submissions from prospective clients still do not meet our checklist of required controls entirely."

2 Sonic Wall Threat Intelligence Confirms Alarming Surge In Ransomware, Malicious Cyberattacks As Threats Double In 2021, February 17, 2022
3 Sonic Wall Threat Intelligence Confirms Alarming Surge In Ransomware, Malicious Cyberattacks As Threats Double In 2021, February 17, 2022
4 Acronis' Mid-Year Cyberthreats Report Finds Ransomware Is The Number-One Threat to Organizations, Projects Damages To Exceed $30 Billion By 2023, August 24, 2022

623 million

The number of ransomware attacks in 2021

Checklist

Ransomware protection – what does good IT security look like?

Ransomware identification:
- Are anti-ransomware toolsets deployed throughout the organization?
- What proactive measures are in place for identification of ransomware threats?
- Are policies, procedures, access controls methods and communication channels updated frequently to address ransomware threats?
- Are in-house capabilities or external arrangements in place to identify ransomware strains?

Business continuity planning/incident response plan:
- Are ransomware-specific incident response processes in place?
- Have there been any previous ransomware incidents? If so, what lessons have been learned?
- Are pre-agreed IT forensic firm or anti-ransomware service provider arrangements in place?

Anti-phishing exercises and user awareness training:
- Is regular user training and awareness conducted on information security, phishing, phone scams and impersonation calls and social engineering attacks?
- Are social engineering or phishing simulation exercises conducted on an ongoing basis?

Backups:
- Are regular backups performed, including frequent backups for critical systems to minimize the impact of the disruption? Are offline back-ups maintained as well?
- Are backups encrypted? Are backups replicated and stored at multiple offsite locations?
- Are processes in place for successful restoration and recovery of key assets within the Recovery Time Objective (RTO)?
- Are backups periodically retrieved compared to the original data to ensure backup integrity?

Endpoints:
- Are endpoint protection (EPP) products and endpoint detection and response (EDR) solutions utilized across the organization on mobile devices, tablets, laptops, desktops etc.?
- Are Local Administrator Password Solutions (LAPS) implemented on endpoints?

Email, web, office documents security:
- Is Sender Policy Framework strictly enforced?
- Are email gateways configured to look for potentially malicious links and programs?
- Is web content filtering enforced with restricting access to social media platforms?

Segmentation:
- Are physical, logical segregations maintained within the network, including the cloud environment?
- Are micro segmentation and zero trust frameworks in place to reduce the overall attack surface?

Monitoring patching and vulnerability management policies:
- Are automated scans run to detect vulnerabilities? Are third party penetration tests performed on a regular basis?
- Does the organization ensure appropriate access policies, enforcement of multi-factor authentication for critical data access, remote network connections and for privileged user access?
- Is continuous monitoring in place for detecting unusual account behavior, new domain accounts and any account privilege escalations (administrator level), new service additions, and unusual chain of commands being run during a short time period?

Mergers and acquisitions:
- What due diligence and risk management activities are performed prior to M&A?
- Are regular security audits conducted on newly-integrated entities to ensure evaluation of security controls?

Rising severity: Double extortion is now the norm

The severity of ransomware claims continues to rise year-on-year as gangs employ increasingly sophisticated attack tools and extortion techniques.

The value of ransomware claims globally has increased significantly since 2019, accounting for well over 50% of all cyber claims costs that AGCS has been involved in together with other insurers over the past two years and remains a significant cost driver through 2022 to date. Business interruption, restoration costs and expert fees are the main loss drivers in a ransomware event.

"The cost of ransomware attacks has increased as criminals have targeted larger companies, critical infrastructure and supply chains," explains **Rishi Baviskar, Global Cyber Experts Leader, Risk Consulting, AGCS**. "Costs have also risen as criminals have honed their tactics and found ways to extort more money from their victims. Double or triple extortion, which can dramatically increase the cost of an attack, is now the norm."

In a traditional ransomware attack, criminals infiltrate a network and use malware to encrypt files, demanding a ransom in return for its restoration. A double extortion attack, however, also involves the theft of sensitive data, which is then used as leverage for extortion. By exfiltrating data, criminals can make ransom demands of companies even if they successfully restore data from backups.

Triple extortion goes one step further, with criminals making extortion demands of business partners, customers, or suppliers that may be affected by data stolen in the initial attack.

Double and triple extortion adds to the cost of a ransomware attack, as well as introducing an element of third-party liability. According to research by CipherTrace[5], double extortion ransomware attacks increased by almost 500% in 2021, while payments to ransomware gangs increased 42% in the first six months to $590m.

Ransomware severity is likely to remain a key threat for businesses, fueled by the growing sophistication of ransomware gangs and rising inflation, which is reflected in the increased cost of IT and cyber security specialists, according to **Marek Stanislawski, Global Cyber Underwriting Lead at AGCS.** "Ransom demands are now tailor-made, with groups investing resources in establishing the 'right' amount and using expert negotiators to maximize their returns.

"Ransomware attackers are becoming more ruthless. As the number of easy targets decreases with improvements in cyber security, they are looking to squeeze more and more profit from successful attacks. Gangs are using a wide range of harassment techniques to successfully extort money."

500%

Double extortion attacks increased by almost 500% in 2021

5 CipherTrace, The Price Isn't Always Right. Ransomware is on the Rise, April 18, 2022

Ransomware costs – double extortion changes the rules and multiplies the cost

Costs description:

Single Extortion

Extortion Payment: demanded by criminals

Lost Income (Business Interruption): The longer period of time in which system accessibility is limited, the greater the loss.

Recovery Expenses: the cost of restoring data and ensuring full systems recovery.

Forensics Expenses: expenses incurred to investigate the source of the security vulnerability.

Double Extortion

Notifications Costs: notifying customers, regulators and other required authorities of a data breach.

Monitoring Costs: monitoring services for identity theft/ fraud that has to be supplied to individuals whose data is stolen.

Regulatory Fines and Legal Expenses: due to third parties' claims whose private data is stolen.

Data Recovery and PR Repairment: Costs of a consultant, crisis management firm or law firm to limit effects of negative publicity.

Sources: Bitsight and Kovrr. Graphic: Allianz Global Corporate & Specialty.

Action on ransom payments on the horizon

High profile disruptive cyber-attacks, such as the 2021 Colonial Pipeline incident[6], has put ransomware on the political agenda, sparking a redoubling of law enforcement efforts. Attention has also turned to the payment of ransom demands, with new rules and potential bans on the horizon.

Ransom demands continue to rise. According to the Paloalto[7] Ransomware Threat Report, ransom demands increased by 144% in 2021, while the average payments rose 78%. Some 46% of companies paid ransoms in order to get data restored, according to Sophos[8]. Manufacturing and utilities, which are particularly vulnerable to extortion, faced the highest ransom payments at an average of $2mn.

The US Treasury stated in 2020 that facilitating ransomware payments to sanctioned hackers may be illegal[9]. EU member states can impose fines for paying ransoms under the Security of Network and Information Systems Directive (NIS Directive). Gartner[10] predicted that by 2025, 30% of nation states will pass legislation that regulates ransomware payments, fines and negotiations, up from less than 1% in 2021.

Last year, the US Treasury Department warned organizations not to breach sanctions rules when paying ransoms. On July 29, 2022, New York State's Department of Financial Services (NYDFS) issued new rules[11] that would require financial services companies to report ransomware incidents and justify extortion payments.

The payment of ransom demands is a contentious topic. Critical service providers, such as hospitals or power companies, may have little option other than to pay a ransom demand in order to avoid crippling disruption. On the other hand, paying extortion demands may encourage further ransomware attacks. Sanction rules and terrorism regulations may also bar payment of ransoms to certain states, groups or individuals, including cyber groups.

Potential legal changes around ransom payments are unlikely to 100% solve the problem of ransomware, but they might help improve the maturity level of companies, according to **Rishi Baviskar, Global Cyber Experts Leader, Risk Consulting, AGCS.** Longer term, cyber criminals are likely to consolidate and change tactics as ransomware attacks become less lucrative, and as easy targets are harder to find.

"Tighter regulation on ransom payments could see cyber criminals shift their focus to other forms of attack, such as data theft or supply chain attacks, as well as more targeted attacks. If ransomware becomes less attractive, they will just look for other ways to monetize cyber-attacks," says **Baviskar.**

Any impacted company should always inform and cooperate with the police or national investigation authorities.

6 Bloomberg, Hackers Breached Colonial Pipeline Using Compromised Password, June 4, 2021
7 Paloalto, 2022 Unit 42 Ransomware Threat Report
8 Sophos, The State Of Ransomware 2022
9 Cynance, Is It Legal To Pay Ransomware Demands?
10 Gartner Unveils The Top Eight Cybersecurity Predictions For 2022-23
11 New York State Department Of Financial Services Proposes Updates To Cybersecurity Regulation

Small and mid-sized companies an increasing sweet spot for hackers

>50%

The average cost of cyber claims for small-business owners rose by more than 50% during the first half of 2022

All companies, across all sectors, are now exposed to ransomware attacks, although small and mid-sized companies are proving a more attractive target for cyber criminals as larger companies beef up their cyber security.

Cyber security, rather than sector focus, is now the key driver for cyber-attacks, explains **Scott Sayce, Global Head of Cyber at AGCS.** "The most attractive targets for cyber criminals traditionally have been large organizations, where they can get the most financial gain for reasonable effort. With these organizations investing heavily in security, the focus is gradually shifting to small and mid-sized firms. The current real sweet spot is a mid-sized business with weak controls, risk management and cyber security in place. That is what cyber criminals like most."

Large companies are better positioned to mitigate the growing threat landscape than smaller companies, which often lack the resources to invest in cyber security and risk management. "Small to medium sized companies see their risks increasing with digitalization, but typically would not carry out impact analysis linked to cyber security and the value of the business," says **Sayce.**

> "Cyber security, rather than sector focus, is now the key driver for attacks

According to managing general agent Coalition, which recently joined Allianz in a multi-year partnership which will see Allianz expand its cyber business for SME and mid-sized companies in key markets, the average cost of cyber claims for small-business owners rose by more than 50% during the first half of 2022 alone[12]: "Across industries, we continue to see high-profile attacks targeting organizations with weak or exposed infrastructure, which has become exacerbated by today's remote working culture and companies' dependence on third-party vendors," it noted. In a similar vein, a study by the German digital association, Bitkom[13], said that the IT systems of medium-sized German companies have been under "heavy virtual fire" this year. At the same time, according to a survey of 1,400 small and mid-sized businesses by the non-profit Cyber Readiness Institute[14], 55% of firms around the world have yet to set up multifactor authentication, which constitutes basic cyber hygiene. Instead, they rely on user names and passwords alone to secure their systems, leaving them vulnerable to preventable cyber-attacks.

That said, even larger companies can have vulnerabilities and blind spots**.** In around 80% of AGCS cyber insurance claims, involving companies with an annual turnover in the triple digit millions, a significant flaw in the security of the insured led, or contributed, to the eventual loss.

"No organization is 100% secure. We know of a recent case in Europe involving a large company with an excellent IT setup, but the attacker found an entry point and compromised their systems. It just takes a software vulnerability, a mistake by an employee, or a supplier with weak controls, and it can result in a large claim. Size and IT maturity will not protect you completely," says **Jens Krickhahn, Practice Leader Cyber Insurance, Central and Eastern Europe at AGCS.**

12 Coalition Releases 2022 Cyber Claims Report: Mid-year Update, September 14, 2022
13 bitkom, 203 Milliarden Euro Schaden pro Jahr durch Angriffe auf deutsche Unternehmen, August 31, 2022
14 The Wall Street Journal, Smaller Companies Are Urged to Adopt Multifactor Authentication, July 5, 2022

BEC incidents rise in the 'deep fake' era

Business email compromise (BEC) attacks have been on the rise, made easier by the growing availability of data, 'deep fakes' and the shift to remote working.

Targeting businesses large and small, BEC attacks can be impactful events, leading to financial loss or more damaging cyber-attacks. BEC attacks can come in different flavors, but typically criminals will use phishing emails and social engineering to steal user credentials or trick an employee to make an unauthorized transfer of funds. BEC is attractive to criminals because they can achieve a big payoff for a relatively low investment of time and resources. Between June 2016 and December 2021, BEC scams globally totaled $43bn, according to the FBI[15]. There was a 65% spike in scams between July 2019 and December 2021 alone.

BEC attacks continue to grow more sophisticated and targeted, with criminals now using virtual meeting platforms to convince victims to transfer funds or to collect information on day-to-day operations. Increasingly, these attacks are supplemented by artificial intelligence (AI) enabled 'deep fake' audio or visuals that mimic senior executives on the telephone or during online meetings.

Last year, criminals used 'deep fake' audio to clone the voice of a company director[16] in order to mislead a UAE bank employee into making a $35mn fraudulent transfer.

Data stolen during double extortion ransomware attacks, and then shared by criminals, is also driving the increase in BEC attacks. Data leak sites offer searchable indexed data that enables cyber criminals to search for specific types of data, enhancing social engineering. According to analysis of ransomware leak sites, Accenture[17] found that an estimated 91% of ransomware victims incurred subsequent data disclosures.

Cyber criminals will continue to evolve their strategy for business email compromise, warns **Tresa Stephens, Head of Cyber, Tech and Media, North America, AGCS.** "We continue to see claims in the US from business email compromise, despite increased awareness of cyber security and efforts to educate employees on phishing. If anything, the risk of attacks is growing. As more and more data is made available online the focus on social engineering and phishing has increased."

$43bn

BEC scams globally totaled $43bn, according to the FBI

15 FBI, Business Email Compromise: The $43 Billion Scam, May 4, 2022
16 Forbes, Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find, October 14, 2021
17 Accenture, How Cybercriminals Are Weaponizing Leaked Ransomware Data For Follow-Up Attacks, August 11, 2022

Geopolitical conflicts reshape threat landscape

$10bn

NotPetya caused an estimated $10bn in damage and business interruption

The conflict in Ukraine, and wider geopolitical tensions, are reshaping the cyber threat landscape. As yet, the war between Russia and Ukraine has not led to a notable uptick in cyber insurance claims, however it does point to a potentially increased risk from nation states.

In addition to an increased risk of espionage, the conflict raises the risk for destructive cyber-attacks against companies with ties to Russia and Ukraine, as well as those in neighboring countries and allies. The spill over of hostilities into cyber space, could see targeted attacks against Western critical infrastructure, supply chains and corporations with the aim of causing physical damage or disruption.

There is particular concern that companies could become collateral damage in any cyber conflict between Russia or Ukraine. In 2017, destructive 'wiper ware' linked to Russia – known as NotPetya – spread to companies around the world, causing an estimated $10bn[18] in damage and business interruption. In addition to the risk of contagious malware, there are also concerns that the tools and techniques used by nation states during the conflict could filter down over time to cyber criminals.

The cyber threat landscape is constantly evolving, says **Jens Krickhahn, Practice Leader Cyber Insurance, Central and Eastern Europe at AGCS:** "We see new exposures and new threats emerging. Six months ago, few people were concerned about a hybrid cyber war, now we see that supporters of Ukraine and Russia have been the targets of cyber-attacks, while critical infrastructure around the world faces an elevated risk. New forms of malicious attack are always to be expected."

18 Financial Times, Insurers must rethink handling of cyber attacks on states, August 29, 2022

Cyber war clauses will provide clarity of cover

Although acts of war are typically excluded from traditional insurance products, the invasion of Ukraine by Russia has accelerated the insurance market's efforts to address the issue of war in cyber wordings and provide clarity of cover for customers.

Cyber risks pose systemic aggregations of exposure, particularly when it comes to war and conflict. A cyber conflict between nations could cause unimaginable damage and disruption to thousands of companies, and potentially whole populations, if attacks target critical infrastructure like utilities, communications or payments systems.

Acts of war are understood in the context of physical damage and personal injury, but cyber war or conflicts are harder to define and difficult to attribute. The lines are increasingly blurred between the actions of nation states, terrorist groups and cyber criminals, while hostilities by nation state threat actors and their affiliates may be clandestine or amount to state-sponsored cyber-attacks that stop short of all-out war.

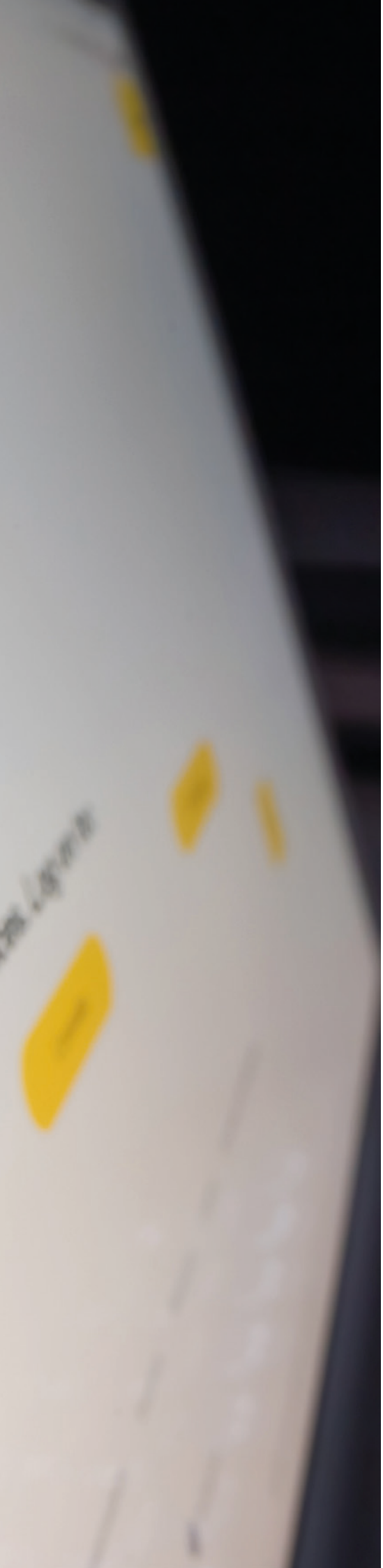
Such events are not without precedent. The 2017 NotPetya contagious malware attack, which affected organizations in more than 60 countries, was attributed by US and UK security agencies to a Russia-backed hacking group. Other high-profile attacks on private companies over the past few years that have been attributed to nation states include Russia's 2020 SolarWinds hack, China's 2021 Microsoft Exchange server breach and Iran's 2021 attack on Boston's Children's Hospital, although in many cases attribution can be very difficult to prove.

The NotPetya attack sparked a debate on cyber war, prompting insurers and brokers to refine contract wordings. A number of standard cyber war exclusions have been developed alongside claims processes to address the issue of coverage and also, in many instances, attribution. The Lloyd's market recently announced it will exclude nation-state cyber-attacks in a bid to limit systemic risk and promote contract clarity.

As the cyber insurance market and product has matured, there is increasing focus on what a cyber war clause should look like.

"We are moving towards more clarity on state-sponsored cyber-attacks," says **Scott Sayce, Global Head of Cyber at AGCS.** "To date, the exclusion for war or state-sponsored attacks in most policies has not been tailored to the cyber product. However, the insurance industry is now in the process of clarifying the intention and phrasing of cyber war clauses, which will remove much of the ambiguity once a claim has occurred."


Sorry, something's gone wrong
We're working hard to fix the problem, please
can still use our other



Business interruption impact

Business interruption is the No. 1 loss driver

Cyber business interruption is the number one digitalization risk of concern for many companies, and the biggest driver for cyber insurance losses overall. According to the **Allianz Risk Barometer 2022**, which asks more than 2,600 risk management experts around the world to identify the top worries for their businesses for the year ahead, cyber incidents and business interruption ranked highest.

57%

Business interruption is the main cost driver for 57% of claims globally

Cyber was also the most feared cause of business interruption, reflecting the rise in ransomware attacks but also vulnerabilities in today's increasingly interconnected world. According to AGCS analysis of cyber-related insurance industry claims that it has been involved with over the past five years, business interruption is the main cost driver for 57% of claims globally and is a significant driver for the rising severity of claims in recent years.

"Digitalization is driving deeper into companies, creating interfaces with customers, suppliers and employees. IT-outsourcing and cloud-usage is more widely and more extensively used. While improving efficiency, these trends also change the threat landscape, creating vulnerabilities as well as increasing interconnectivity and aggregations of risk," **says Michael Daum, Global Head of Cyber Claims at AGCS.**

Industrial Control Systems: manufacturing's Achilles' heel

Over the past five years, manufacturing and industrial companies have joined the ranks of retailers, financial institutions and healthcare providers as the targets of cyber-attacks.

Hackers now actively target manufacturing and critical infrastructure companies, where IT infrastructure and cyber security is not as strong. Cyber-attacks against manufacturing and critical infrastructure companies also involve longer business interruption recovery times and can directly affect consumers, giving cyber criminals additional leverage when it comes to extortion demands.

In particular, industrial and manufacturing companies that use industrial control systems are particularly vulnerable to cyber-attacks, especially where older systems are connected to networks.

"Industrial control systems are the Achilles' heel of manufacturing and production companies," **explains Rishi Baviskar, Global Cyber Experts Leader, Risk Consulting, AGCS.** "Many systems have worked well in isolation for decades, but since the pandemic, more and more companies are connecting systems which include 'end of life' network components to their networks for remote monitoring and/or control. But 'end of life' systems are not secure and can expose companies to cyber-attacks, including ransomware, if they are not segregated and well-protected from the rest of the network."

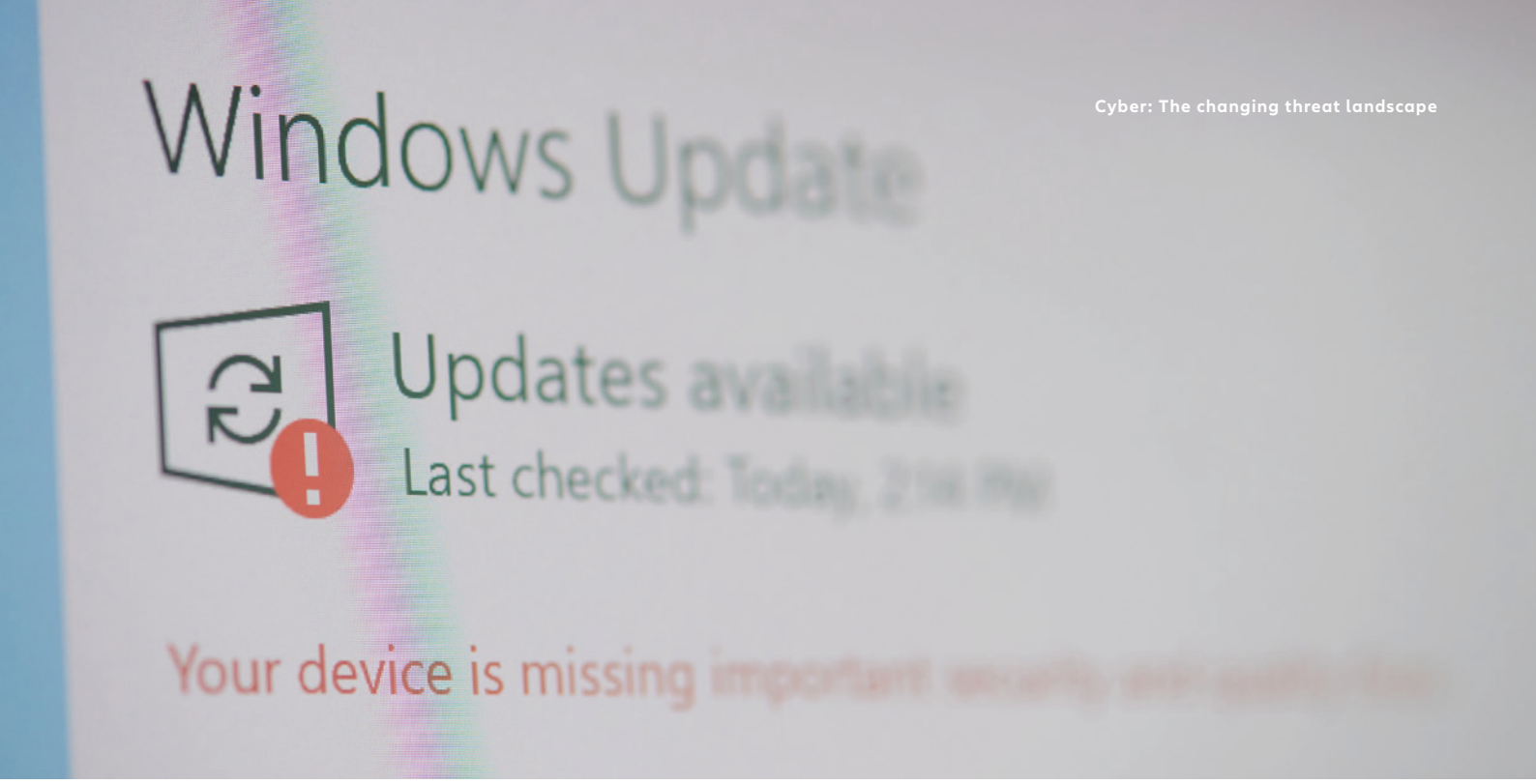
Cyber business interruption can be caused by a wide range of triggers, including a malicious cyber-attack, a software or hardware glitch, human error or a disruption to third party IT infrastructure or services, such as a power or cloud outage. However, skyrocketing ransomware attacks in recent years have also thrust business interruption into the limelight – this is the largest loss driver for cyber insurance claims in Europe. Some 90% of cyber claims are first party, of which 80% are from ransomware. Business interruption losses can be as much as seven times extortion demands, based on claims AGCS has seen.

Notably, ransomware incidents have seen business interruption overtake third -party liability as the main source of loss in the US, where the cyber insurance market has historically been driven by data breaches.

"Business interruption related expenses have overtaken data breach related expenses as the largest driver of costs incurred after a cyber incident," confirms **Tresa Stephens, Head of Cyber, Tech and Media, North America, AGCS.**

If a ransomware attack or an IT outage is not rectified quickly, business interruption losses quickly mount. Manufacturing and industrial companies are particularly exposed to such business interruption losses as it can take weeks or even months to restore production levels from just a small outage. A cyber-BI incident at a major supplier could also ripple through the value chain, causing contingent business interruption (CBI) losses for customers and suppliers around the world.

Contingent business interruption is a particularly difficult area for risk transfer, **according to Michael Daum, Global Head of Cyber Claims at AGCS**. "CBI cover comes with a key challenge, especially for non-IT providers. It is not clear whether the insured, and subsequently the insurer, will have access rights to determine what has happened at the third party. Ultimately, the insurer will need to have the evidence in place that a network intrusion has happened, and the cyber policy is triggered," **says Daum.**



Hackers zero in on vulnerable supply chains and M&A

Another worrying development is the deliberate targeting of supply chains, both traditional and digital. Such attacks are a particular concern for the insurance market, as a single cyber-attack can trigger losses at potentially thousands of companies around the globe.

Supply chain attacks have emerged as a significant risk in recent years, in part a reflection of the growing sophistication of ransomware attacks. Cyber criminals are targeting supply chains, which are already under pressure since the pandemic, and where they may have additional leverage. They are also targeting smaller critical suppliers within supply chains as well as suppliers that are in the process of a merger or acquisition, in order to gain access to the larger acquiring firm.

Last year, the Colonial Pipeline[19] – which distributes fuel to the US East coast, was hit by a ransomware attack that shut down the pipeline. Hackers are also targeting software supply chains, inserting malware into legitimate software. The 2021 ransomware attack against cloud-based MSP platform Kaseya[20] affected some 1,500 companies via malware inserted into a software update.

According to IBM[21], manufacturing overtook financial services to become the most attacked industry in 2021, as ransomware gangs used the threat of supply chain disruption to pressure firms into paying ransoms. Almost half (47%) of attacks on manufacturing were due to unpatched vulnerabilities.

Manufacturers are particularly vulnerable to cyber-attacks through their supply chains, which can be complex and involve thousands of suppliers. While many large companies have taken measures to reduce the risk of ransomware attacks, cyber security maturity and transparency throughout the supply chain is still largely absent, while cyber risk management among small- to medium-sized companies is lagging.

"Organizations need to be careful not to create gaps in cyber security in their supply chains or when outsourcing. The safe use of cloud services requires distinct security knowledge, which organizations need to build first," says **Michael Daum, Global Head of Cyber Claims at AGCS.** "It is a common misconception that the outsourcing or cloud vendor will assume full responsibility."

47%

Almost half (47%) of attacks on manufacturing were due to unpatched vulnerabilities

19 Bloomberg, Hackers Breached Colonial Pipeline Using Compromised Password, June 4, 2021
20 Reuters, Up To 1,500 Businesses Affected By Ransomware Attack, U.S. Firm's CEO Says, July 6, 2021
21 IBM Report: Manufacturing Felt Brunt Of Cyberattacks In 2021 As Supply Chain Woes Grew, February 23, 2022

Cloud outsourcing: Accumulating risks for the future

Companies continue to shift their services and data storage onto the cloud, despite growing concerns around security and aggregations of risk.

According to the 2022 Thales Cloud Security Report[22], two thirds (66%) of organizations store 21%-60% of their sensitive data in the cloud. However, 45% say they have experienced a data breach or failed an audit involving data and applications in the cloud, up on the 35% reported in 2021. The three largest cloud providers, Amazon, Microsoft and Google, account for 65%[23] of the worldwide market for cloud services.

By concentrating risk into a small number of IT service providers, software vendors and platforms, businesses may be storing up problems for the future, **warns Tresa Stephens, Head of Cyber, Tech and Media, North America, AGCS.** "By relying on a small number of providers for cyber security or cloud services, society is creating large aggregations centered around single points of failure. Outsourcing to tech solutions providers may help, but these concentrations of exposure need to be carefully considered and underwritten."

Cyber-attacks, outages or software bugs could take cloud services and internet infrastructure offline for hours or days, causing business interruption for thousands of companies.

"Ultimately every company is responsible for cyber security, and that is often forgotten, especially with outsourcing and the move to the cloud. Each company needs to ensure that adequate controls and processes are in place, and this is often not the case," says **Marek Stanislawski, Global Cyber Underwriting Lead at AGCS.**

22 Cloud Data Breaches and Cloud Complexity on the Rise, Reveals Thales, June 7, 2022
23 CRN, Top Cloud Market Share Leaders: AWS, Microsoft, Google Lead Q2 2022, August 17, 2022

Third-party liability

Exposures continue to evolve

Cyber-related third-party liability exposures continue to evolve with technology and regulation creating new exposures.

Third party liability is becoming more relevant with advances in technology, as organizations and connected devices collect a growing volume of personal data, including information on health, behavior and biometrics. At the same time, artificial intelligence (AI) and powerful analytics enable organizations to process data and make decisions or provide advice in real time, such as with chatbots and automated services.

Data breach and privacy regulations continue to expand, following the introduction of tough rules in Europe under the General Data Protection Regulation (GDPR), and more stringent regulations in locations and countries such as California, Brazil, China and India. In addition, a number of US states have passed biometric privacy laws, while the EU is developing a regulatory framework on AI. Through 2023, government regulations requiring organizations to provide consumer privacy rights will cover five billion people worldwide, representing more than 70% of global GDP, and up on around three billion people in 2021, according to Gartner[24].

Almost any cyber incident can lead to litigation or demands for compensation from affected customers, suppliers and data breach victims, according to **Tresa Stephens, Head of Cyber, Tech and Media, North America, AGCS.**

As technology evolves, it tends to be regulated on the backend as the drawbacks inherent in new advancements come to light, Stephens explains. For example: technological advancements and the move to online business models have altered the ease with which companies can gather, store and share consumer data. Social media companies mined users' data for years, often without their knowledge of what the data was ultimately being used for. As consumer privacy rights became an area of increased concern, regulators have responded with regulations.

Third party liability losses are also becoming more important for ransomware claims, where losses are typically driven by business interruption and restitution costs. The rise of double extortion ransomware attacks, where criminals steal and use personal data, can give rise to data breach claims and litigation.

"Most ransomware incidents today go along with data breaches and impose a significant risk for companies with personal or sensitive data. Third party liability, as well as fines and penalties, are likely to become more relevant with evolving data protection and privacy legislation and as hackers increasingly employ double and triple extortion techniques," says **Michael Daum, Global Head of Cyber Claims at AGCS.**

70%

Through 2023, government regulations requiring organizations to provide consumer privacy rights will cover five billion people worldwide, representing more than 70% of global GDP

24 Gartner Unveils The Top Eight Cybersecurity Predictions For 2022-23

ESG

Cyber security increasing seen through the environmental, social, and governance lens

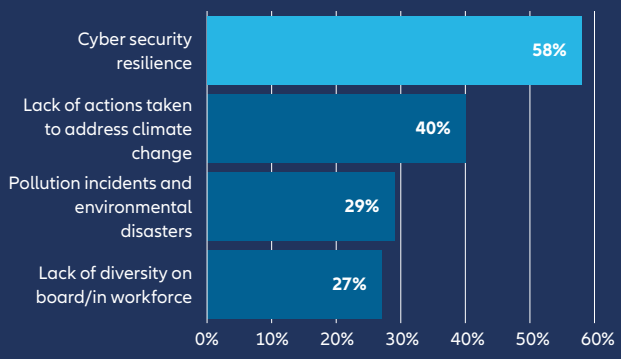
Cyber security has long been seen as an IT issue but today's booming digital economy means this is no longer the case. Whether it's the rise of home working, the acceleration of digitalization, or the far-reaching effects of events such as the ransomware attack on the Colonial Pipeline[25] in the US, the potential and actual vulnerabilities exposed by cyber incidents have become all too apparent, ensuring a far broader demographic is increasingly concerned with cyber security's social impact, including company management, global investors and stakeholders with potential exposure to customers' private information.

Indeed, cyber security resilience is now regarded as the major ESG risk topic for many companies, according to the majority of respondents in the **Allianz Risk Barometer 2022** (58%) *(see graphic)*. This is driven by factors such as the growth and severity of cyber-attacks, and the introduction, and increase, of data security regulations to enhance the protection of personal information around the world. Given companies can be fined and/or suffer reputational damage if they do not adequately protect their information/networks, there is growing acknowledgment of the need to build resilience and plan for future outages or face the consequences from regulators, investors and other stakeholders.

25 Bloomberg, Hackers Breached Colonial Pipeline Using Compromised Password, June 4, 2021

Which ESG risk trends are of most concern to your company?

Top four answers



Source: Allianz Risk Barometer 2022

Figures represent the percentage of answers of all participants who responded (2,650). Figures do not add up to 100% as up to three risks could be selected.

> The potential and actual vulnerabilities exposed by cyber incidents have become all too apparent, ensuring a far broader demographic is increasingly concerned with cyber security's social impact

In the past, it was mainly technology companies that were assessed on cyber security resilience, but these days, businesses across a range of sectors are subject to such scrutiny. Increasingly, cyber security considerations are incorporated into the ESG risk-analysis frameworks of data providers, who look into companies' data protection and information security practices to evaluate their preparedness for cyber crime while investors typically examine data protection and information security policies to assess a firm's cyber security risks.

Making sure a company's cyber security processes and policies are understood at the board level and that cyber risk monitoring processes are in place is crucial. One of the main complaints from the investment community has been around transparency – it is hard to understand a company's cyber risks and for various reasons companies have been slightly hesitant in the past to provide enough transparency. But the ones that do certainly see the benefit.

Considering cyber security as an ESG metric is still a relatively new concept but continued and expanded interest in this area is to be anticipated. Companies that don't recognize these changes and don't integrate their ESG and cyber security strategies may discover that they have a lot more to deal with than just a cyber insurance claim in future.

Talent

Shortage of cyber security pros

A shortage of cyber security professionals may be hindering efforts to improve cyber security, especially outside the technology sector.

Demand for cyber security experts is growing at a time of constrained labor supply in the US and Europe. More and more companies are looking to employ cyber security specialists, but supply is not keeping up with demand. According to Cybersecurity Ventures[26], the number of unfilled cybersecurity jobs worldwide grew 350% between 2013 and 2021 to 3.5 million – enough to fill 50 large football stadiums.

Board awareness of cyber has accelerated security investment in recent years, but many companies struggle to get the IT professionals required to implement changes at the required pace and scale, according to **Jens Krickhahn, Practice Leader Cyber Insurance, Central and Eastern Europe at AGCS.**

"Just two or three years ago there was a lack of awareness of cyber among top management, but that has changed dramatically with large supply chain cyber-attacks, and more recently with the changing threat landscape from the conflict in Ukraine. As a result, the C-Suite are more engaged with cyber risk and have stepped up investment," says **Krickhahn.**

"However, the problem is now one of talent," adds **Michael Daum, Global Head of Cyber Claims at AGCS.** "There is a global shortage of cyber security professionals, and many companies are experiencing problems hiring, which has affected the ability of some companies to make improvements to cyber security."

26 CyberSecurity Ventures, Cybersecurity Jobs Report: 3.5 Million Openings In 2025, November 9, 2021

A sustainable cyber market

The cyber risk management partnership

Following a rise in ransomware losses in 2020 and 2021, the insurance industry is more diligently assessing clients' cyber risk profiles in a bid to incentivize companies to improve cyber security and risk management controls.

By increasing cyber security, companies are less attractive to attackers, according to **Jens Krickhahn, Practice Leader Cyber Insurance, Central and Eastern Europe at AGCS.** "Generally, it is not commonplace for us to see clients with strong cyber maturity and security mechanisms suffer a high frequency of 'successful' attacks. Even where they are attacked, losses are typically less severe due to established identification and response mechanisms. It is clear that organizations with good cyber maturity are better equipped and prepared to deal with these incidents."

Incident response is critical, as the cost of a claim quickly escalates once business interruption kicks in, according to Krickhahn. "You can build a high defensive wall, but that is not guaranteed to hold. You will also need test plans and measures in place to deal with an incident, including a crisis management team and a network of professional support partners. This will help to keep claims as small as possible. A win-win situation for everyone. The higher the maturity of IT security in a company, the lower the percentage of customers with damage or prior damage."

Ransomware losses have changed the industry's approach to cyber risk for the better, encouraging cooperation between insurers and clients on cyber risk management and mitigation, according to **Tresa Stephens, Head of Cyber, Tech and Media, North America, AGCS.** "We wanted to really get under the hood of our insureds and help them with more insightful information on how to protect themselves and mitigate cyber risks. It's now night and day from where we were just three years ago," says **Stephens.**

"There is also now a very different conversation on the quality of cyber risk. We are getting much better insights, while the insurance industry is providing more value. For example, through collaboration with our trusted partners and our in-house specialist risk consultants, we can offer useful information and advice to customers, such as which controls are most effective, as well as provide risk management and response services. The net result in the future should be fewer successful or significant cyber events for our customers."

Insurers' recommendations place a "value" on cyber security investment, explains **Michael Daum, Global Head of Cyber Claims at AGCS.**

"We make sure that the 'digital sprinklers' are installed. Risk engineering and underwriting recommendations are now a pre-requisite to obtaining cyber insurance. While these recommendations clearly make sense, increasingly we see that insurance is the catalyst to get cyber security measures implemented today, rather than in two or three years' time."

Based on AGCS underwriting and risk engineering questionnaires, a number of companies still need to improve their frequency of IT security training; network segmentation for critical environments; and clean patch management in particular. Companies' cyber incident response plans and cyber security governance are among the weakest areas.

Stephens advises companies to engage with their insurers early and have concrete plans to address gaps in cyber security: "We do see this as a partnership. By asking the right questions in advance you can identify vulnerabilities and gaps and address them ahead of renewal. It pays to have that conversation early and often."

Working towards a sustainable cyber insurance product

$20bn

Cyber insurance premiums worldwide are expected to increase to well-over $20bn by 2025

Demand for cyber insurance remains strong, but market factors and weak cyber security in some sectors are limiting growth opportunities.

In response to a spike in ransomware losses, and growing awareness of systemic, and aggregations of, cyber risk, capacity in the market has become constrained, while premiums have increased. Many insurers have also tightened underwriting criteria, requiring insureds to maintain minimum levels of cyber security and controls.

There are still many companies out there with vulnerabilities and lacking security controls that will struggle to purchase cyber insurance in this market, according to **Marek Stanislawski, Global Cyber Underwriting Lead at AGCS.** "There is adequate capacity for well-managed companies that have a proper understanding of their cyber risk profile and that have appropriate controls and security in place."

Many customers continue to receive broad cover for a wide range of exposures, including third party liability and business interruption, explains **Tresa Stephens, Head of Cyber, Tech and Media, North America, AGCS.**

"The cyber insurance market has undergone a correction, but deep-rooted issues remain, such as systemic risks and aggregations of exposure. There also continues to be a delta between the drivers of exposure and mitigation. We need to get to a place where the cyber insurance market is sustainable. The more we partner with our clients and help them adjust to the threat landscape, the more losses will hopefully reduce."

The insurance industry has an important role to play in improving cyber security, explains **Stanislawski:** "We want to be a partner for cyber insurance in the long term. Cyber has the potential to become one of the most important insurance policies a company purchases, given it is one of the biggest threats most companies face today and in the future.

"Business will need a risk transfer solution for cyber and that is why we continue to adjust our underwriting and work hand-in-hand with clients to improve cyber security maturity."

Insurers have a role that goes beyond pure risk transfer, helping clients adapt to the changing risk landscape and raising their protection levels, explains **Michael Daum, Global Head of Cyber Claims at AGCS.**

"Cyber will become a well-established insurance product. The market and the cyber product is maturing, and we increasingly see a consensus on what good cyber security maturity looks like and what can and cannot be covered by insurance," Daum concludes.

According to Munich Re, at the beginning of 2022, cyber insurance premiums worldwide totaled in excess of $9bn. This is expected to increase to well-over $20bn by 2025[27], a figure also predicted by AGCS in its first cyber risk report in 2015.

27 Munich Re, Cyber Insurance: Risks and Trends 2022

Growing interest in captives and ART

Purchasing habits for cyber insurance have been shifting with the evolving risk landscape and the challenging market for cyber insurance.

Following large ransomware losses, cyber insurance premium rates have increased over the past two years, and underwriting criteria has tightened. In some cases, organizations have not been able to buy the limits or programmes they previously did. As a result, many buyers of cyber insurance have considered alternative programme structures and alternative risk solutions for cyber.

Captives are often used as a tactical complement to increase coverage and fill in gaps in coverage and after recent ransomware attacks and other cyber losses, an increasing number of companies are looking at how they can utilize captives to both benefit their finances and protect their organization.

"Generally, retention levels have increased, and companies now have more skin in the game. As a result, we have seen more interest in the use of captives and virtual captives for cyber," **Jens Krickhahn, Practice Leader Cyber Insurance, Central and Eastern Europe at AGCS** confirms.

In the US **Stephens** agrees that retentions have also increased considerably, and demand for limit is being tempered by the cost of insurance. As a result, many companies are looking for ways to get the most out of their cyber insurance and fund higher retentions: "We are having more conversations with clients on alternative risk transfer solutions for cyber, including fronted policies and tailored structured solutions."

Contacts

For more information contact your local Allianz Global Corporate & Specialty Communications team.

Asia Pacific
Shakun Raj
shakun.raj@allianz.com
+65 6395 3817

Ibero/LatAm
Camila Corsini
camila.corsini@allianz.com
+55 11 3527 0235

North America
Sabrina Glavan
sabrina.glavan@agcs.allianz.com
+1 973 876 3902

UK and Nordics
Ailsa Sayers
ailsa.sayers@allianz.com
+44 20 3451 3391

Central and Eastern Europe
Daniel Aschoff
daniel.aschoff@allianz.com
+49 89 3800 18900

Mediterranean/Africa
Florence Claret
florence.claret@allianz.com
+33 158 858863

Lesiba Sethoga
lesiba.sethoga@allianz.com
+27 11 214 7948

Global
Hugo Kidston
hugo.kidston@allianz.com
+44 203 451 3891

Heidi Polke-Markmann
heidi.polke@allianz.com
+49 89 3800 14303

For more information contact agcs.communication@allianz.com

Follow Allianz Global Corporate & Specialty on

Twitter **@AGCS_Insurance** and

LinkedIn

www.agcs.allianz.com

Allianz Global Corporate & Specialty SE

Dieselstr. 8, 85774 Unterfoehring, Munich, Germany

Images: Adobe Stock

October 2022