MANAGING THE IMPACT OF INCREASING INTERCONNECTIVITY: TRENDS IN CYBER RISK

ALLIANZ GLOBAL CORPORATE & SPECIALTY

Allianz

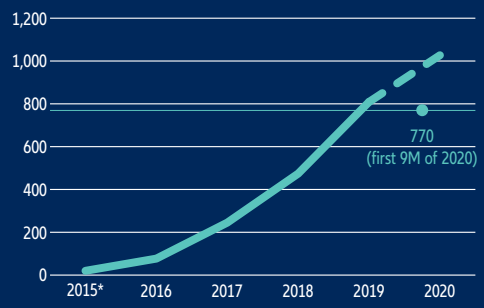
72%
increase in the average cost of cyber crime to an organization in five years to
US$13mn*

67%
increase in the average number of security breaches in five years*

*Accenture/Ponemon, The Cost of Cyber Crime

ANALYSIS: INSURANCE CLAIMS

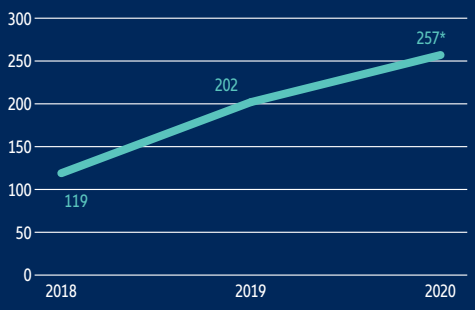
NUMBER OF CYBER-RELATED CLAIMS
PER YEAR



*AGCS only started offering cyber insurance in 2013, so claims experience is limited

Source: Allianz Global Corporate & Specialty

AVERAGE NUMBER OF CLAIMS
PER QUARTER



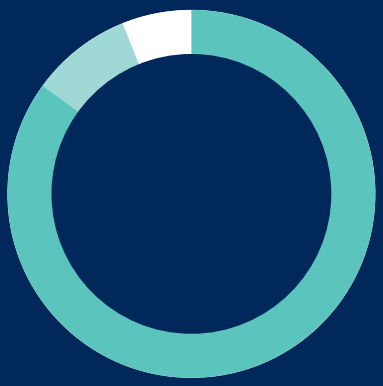
based on first 9M of 2020 only

There has been a notable rise in cyber-driven claims in recent years, driven by the growth of the cyber insurance market but also by the rise in incidents such as data breaches, distributed denial of service attacks, phishing campaigns, and increasingly, ransomware events. Human error and technical failures are also major drivers.

A growing **"commercialization of cyber-hacks"** is a contributing factor leading to a growth in ransomware claims in particular *(see page 6)*. Increasingly, criminals are selling malware to other attackers who then target businesses demanding ransom payments, meaning high-end hacking tools are more widely available and cheaper to come by.

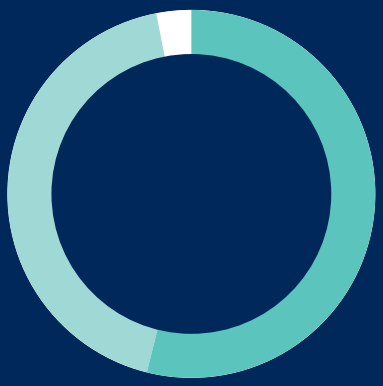
While the Covid-19 outbreak cannot be said to be a direct cause of cyber-related claims, exposures have been rising during the pandemic, particularly with regards to ransomware and business email compromise incidents, given the increase in remote working and the likelihood that security safeguards may not be as robust in the home office. Although AGCS has seen the first few cyber claims which can be indirectly attributed to the Covid-19 shift in the business landscape, it is too early to tell whether this is a broader trend.

CAUSE OF LOSS BY VALUE OF CLAIMS



- **External manipulation of systems** (e.g. direct attack from the internet or malicious content such as ransomware/malware) **85%**
- **Malicious internal action** (e.g. action taken by a rogue employee) **9%**
- **Accidental internal cause** (e.g. human error, technical/systems failure or outage) **6%**

CAUSE OF LOSS BY NUMBER OF CLAIMS



- **Accidental internal cause** (e.g. human error, technical/systems failure or outage) **54%**
- **External manipulation of systems** (e.g. direct attack from the internet or malicious content such as ransomware/malware) **43%**
- **Malicious internal action** (e.g. action taken by a rogue employee) **3%**

Based on analysis of 1,736 claims worth €660.4mn (US$ 770mn) reported from 2015 until September 2020. Total includes the share of other insurers involved in the claims in addition to AGCS.

Source: Allianz Global Corporate & Specialty

Losses resulting from the external manipulation of computer systems such as distributed denial of service attacks (DDoS) or phishing and malware/ransomware campaigns account for the significant majority of the value of claims analyzed. Cyber-crime generates the headlines but the analysis also shows that more mundane technical failures, IT glitches or human error incidents are the most frequent generator of claims, although, overall, the financial impact of these events is, on average, limited compared with external events.

Whether it results from an external cyber-attack, human error or a technical failure, **business interruption is the main cost driver behind cyber claims. It accounts for around 60% of the value of all claims analyzed**, with the costs associated with dealing with data breaches ranking second.

TRENDS

Cyber claims growing in number and complexity

External attacks cause most expensive losses. Internal accidents occur more frequently

Business interruption main cost driver behind claims

Remote working and Covid-19 heightening exposures

Ransomware incidents more frequent and financially-damaging

Business compromise email attacks surge

Costs of "mega" data breaches increasing

Regulatory exposure increasing around the globe

Class action litigation on the rise

M&A brings cyber risk

Nation state-sponsored attacks on the rise

OVERVIEW

Just seven years ago cyber risk ranked as low at 15th in the **Allianz Risk Barometer**, an annual survey in which more than 2,700 risk experts from 100 countries identify the top threats for companies for the next 12 months and beyond.

Today, it ranks either near or at the top of seemingly every risk poll conducted. In the intervening years both knowledge of the threats posed to businesses by cyber and the number of related claims or losses have increased significantly. At the same time, businesses and their insurers now have to deal with a fast-changing, ever-evolving risk landscape, which has been further exacerbated by the outbreak of the coronavirus pandemic.

Companies are facing a number of challenges: such as the prospect of more disruptive and expensive business interruptions, the increase in the frequency and cost of ransomware incidents, the consequences from larger data breaches and more robust regulation – both at home and overseas – as well as the prospect of litigation if something does go wrong. The playing out of political differences in cyber space also ups the ante while even a successful merger and acquisition (M&A) can bring unexpected problems. Then, there is the fact that many employees are now working remotely. Displaced workforces create new opportunities for increasingly better organized and funded cyber criminals to exploit and gain access to networks and sensitive information. At the same time the potential impact from human error or technical failure incidents – already one of the most frequent drivers of cyber claims – may also be heightened. Employers and employees must work together to raise awareness and increase cyber resilience in the home office set-up.

Despite the huge advances companies have made in cyber risk awareness in recent years, many are still playing catch-up and often do not realize how important their digital assets are until something happens. This report highlights some of the most significant cyber risk trends currently occupying the attention of insurers, risk managers and their broker partners and how companies can be better prepared to mitigate the impact of such incidents.

LAXER SECURITY POST COVID-19 HEIGHTENS CYBER RISK

Rise in scammers and spammers looking to exploit vulnerabilities, as pandemic enhances existing threats and problems

The coronavirus outbreak has resulted in the largest work-from-home situation in history, presenting criminals with new opportunities to exploit any security vulnerabilities created by the pandemic.

With many companies having expanded their remote working capacity through the outbreak – often at very short notice – in order to provide as many employees as possible with easy access to software and systems, IT security standards may have had to be lowered or suspended, putting cyber security under new levels of stress. According to research by cyber security firm Arceo almost all of the CISOs at 250 companies, with $250mn to $2bn in annual revenue[1], believe that security practices when working remotely are unlikely to be as stringent as those at the office.

One consequence of potentially laxer security may be that cybercriminals and hackers may find it easier to penetrate previous effectively-protected corporate systems, causing data breaches, cyber blackmail intrusions and IT system failures. Those CISOs stated that cloud usage, personal device usage and unvetted apps or platforms pose the biggest threats during this work from home period. At the same time, it is estimated that anywhere between 50% and 90% of data breaches are caused or abetted by employees, be it by simple error or by falling victim of phishing or social engineering.

Through 2020, malware and ransomware incidents have already increased by more than a third, at the same time as a 50%+ increase in phishing, scams, and fraud, according to international police body, INTERPOL. The rush to adopt new cloud systems and remote access solutions, has also driven up the number of data breaches. Over a four-month period, some 907,000 spam messages, 737 incidents related to malware and 48,000 malicious URLs[2] – all of them in relation to coronavirus– were detected by one of INTERPOL's private sector partners.

Specific sectors have also reported a rise in incidents. In the US, with millions of Americans now working from home – including those charged with looking after critical infrastructure – cyber-attacks on the electric grid have surged by 35% during the pandemic[3]. In a worst case scenario, such attacks could trigger blackouts or damage vital equipment. In May, the UK's grid data system was hacked, although electricity supplies weren't affected. And in March, an attack against Europe's association of grid operators, ENTSO-E, affected its internal office systems. In the maritime and offshore energy sector there have been reports of a 400% increase in attempted cyber-attacks since the pandemic began.

To date, AGCS has only seen a small number of cyber claims which are Covid-19 related, however a further increase in cyber crime is likely in the near future as criminals continue to ramp up their activities and develop more sophisticated techniques.

Business email compromise schemes *(see page 7)* are likely to increase further with the shift in the business landscape to remote working and the economic downturn, along with damage costs from phishing scams, ransomware attacks and insecure remote access to networks. Coronavirus-themed online scams and phishing campaigns which aim to take advantage of public concern about the pandemic are unlikely to dissipate anytime soon.

The pandemic will also have a long-term impact as companies increasingly digitalize, work remotely and rely more on online sales in response, meaning cyber risks will evolve in different shapes and forms.

"MALWARE AND RANSOMWARE INCIDENTS HAVE INCREASED BY MORE THAN A THIRD"

1 Arceo, Building Cyber Resilience, The 2020 CISO Perspective

2 Interpol, Report Shows Alarming Rise of Cyber-Attacks During Covid 19, August 2020

3 Bloomberg, Hackers Are Tackling The Remote Workers Who Keep Your Lights On, July 2020

2 BUSINESS INTERRUPTION AND DIGITAL SUPPLY CHAIN VULNERABILITY GROWING

Digital disruption has become a much more significant driver of cyber losses while cyber risk in supply chains is a growing exposure, given the increasing reliance on technology

Business interruption (BI) following a cyber incident has become a major concern for business. Analysis of cyber claims by AGCS shows that BI is the main cost driver in the majority of cases. Whether ransomware, human error or a technical fault, the loss of critical systems or data can bring an organization to its knees in today's digitalized economy.

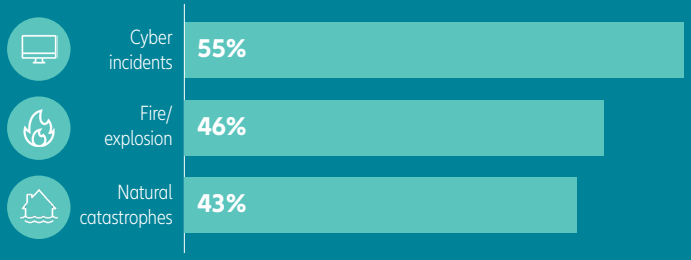
Cyber and BI now rank as the top two risks for companies respectively, according to the **Allianz Risk Barometer 2020**, which was conducted before the coronavirus outbreak – and are increasingly interrelated. Awareness has been growing following high profile outages across a number of sectors, including banking and airlines. At the same time, ransomware attacks, such as the 2017 **NotPetya** malware and the **Ryuk** campaign, have caused serious disruption for manufacturing and service sectors, as well as public sector organizations.

Loss of data, or "business intelligence", is emerging as a major cause of loss. The inability to access data for an extended period of time can have a significant impact on revenues – for example, if a company is unable to take orders. One notable large BI claim in 2019 involved a fire at a European media company. A significant proportion of the claim was related to the unavailability of data and the cost of restoration.

Dependency on digital supply chains – both for the delivery of services and the supply of goods – brings numerous benefits. Shared technology-based platforms enable data to be exchanged between parties, automates administrative tasks and orders and transports products on demand. However, such platforms can potentially create a chain reaction ensuring a BI cascades through a whole sector. If a platform is unavailable due to a technical glitch or cyber event, it could bring large BI losses for multiple companies that all rely and share the same system. In June 2019, an outage caused a catastrophic failure at some Google cloud services, causing several hours of disruption to a number of large online service providers, including You Tube, Uber and Snapchat. In 2017, a four-hour outage at Amazon Web Services in North America was estimated to have cost S&P 500 companies $150mn.

As recently as five years ago, the cyber claims teams at insurers such as AGCS focused primarily on data breaches and resulting first party damage and liability. But with the growing reliance on technology, interest in first party and BI covers has increased, meaning the claims function increasingly represents an interdisciplinary team, with expertise in business continuity and forensic accounting.

ALLIANZ RISK BAROMETER: WHICH CAUSES OF BUSINESS INTERRUPTION ARE FEARED MOST BY COMPANIES?



Source: Allianz Global Corporate & Specialty. Figures represent the percentage of answers of all participants who responded (1,018). Figures don't add up to 100% as up to three risks could be selected.

3 RANSOMWARE NOW THE MOST PROMINENT CYBER-CRIME THREAT

Incidents are becoming more frequent, sophisticated and financially damaging

Ransomware attacks are increasingly becoming one of the biggest causes of cyber loss. In fact the EU's law enforcement agency, EUROPOL, now regards them as the most prominent cyber-crime threat.

Already high in frequency, incidents are becoming more damaging, increasingly targeting large companies with sophisticated attacks and hefty extortion demands. Five years ago, a typical ransomware demand would have been in the tens of thousands of dollars. Now they can be in the millions.

The consequences of an attack can be crippling, especially for organizations that rely on data to provide products and services, but it can also create significant damage for others in the supply chain, such as critical infrastructure.

There were nearly half a million ransomware infections reported globally last year, costing organizations at least $6.3bn in ransom demands alone, according to estimates from security vendor Emsisoft[4]. Total costs associated with dealing with these incidents are estimated to be well in excess of $100bn. Extortion demands are just one part of the picture. Business interruption (BI) can bring the most severe losses from ransomware attacks – with downtimes becoming longer – and the costs associated with systems and data restoration can be huge. A breakdown of a recent insurance industry cyber loss in Europe shows that the restoration and expenses costs were similar to the ransom demanded. Meanwhile, the BI proportion of the loss was four to five times greater.

In some cases, ransomware is a smoke screen for the real target, such as the theft of personal data. Between January and June, 2020, ID Ransomware[5] received 100,001 submissions relating to attacks by ransomware groups that target companies and public sector organizations. Of these 11,642 related to attacks by the groups that overtly steal data – around 11% – the real figure is probably higher.

Attacks have also evolved beyond the scattergun high-volume phishing attacks seen in previous years with well-funded organized gangs of cyber criminals launching more complex and targeted attacks against large companies, which can command high ransom demands.

Incidents such as those featuring the **Ryuk malware**, and the attack on global aluminum producer Norsk Hydro in 2019 which meant its workforce had to resort to pen and paper, have emerged as a key driver for cyber insurance claims in recent years. Ryuk was first reported in August 2018 and has been responsible for multiple attacks against large companies, hospitals and local governments globally. Such attacks are well planned, with hackers taking the time to identify and target critical network systems, therefore maximizing the impact of the attack and the value of demands.

More ransomware and extortion attacks can be expected in future with the post-Covid-19 landscape exacerbating this threat, given the increasing number of people working at home and the fact that safeguards may not be as good at home as in the workplace. Reported malware and ransomware incidents have already believed to have increased by more than a third since the start of 2020.

The **"commercialization of cyber-hacks"** is also leading to more incidents. Increasingly, cyber criminals are adopting "franchise" models and are selling malware to other attackers who then target businesses demanding ransom payments. This is making high-end hacking tools more widely available to exploit online vulnerabilities.

"BUSINESS INTERRUPTION CAN BRING THE MOST SEVERE LOSSES FROM RANSOMWARE ATTACKS AND THE COSTS ASSOCIATED WITH SYSTEMS AND DATA RESTORATION CAN BE HUGE"

4 Emsisoft, Infosecurity Magazine, Ransomware Costs May Have Hit $170bn in 2019, February 13, 2020

5 ID Ransomware

4 BUSINESS EMAIL COMPROMISE ATTACKS SURGING

Economic downturn and shifting landscape resulting in more incidents

Business email compromise (BEC) – or spoofing – attacks have been increasing in frequency for some time and will likely further surge in future due to the economic downturn and shift in the business landscape driven by the coronavirus outbreak. More people working from home means new opportunities for criminal activities are generated. Prior to the pandemic, BEC incidents had already resulted in worldwide losses of at least $26bn since 2016, according to the FBI. Between May 2018 and July 2019, the number of incidents discovered worldwide doubled, with the average economic loss around $270,000.

A BEC attack typically involves social engineering and phishing emails to dupe employees or senior management at companies into revealing login credentials or to make fraudulent transactions. Over time, BEC attacks have grown in sophistication, with criminals now using compromised email and spoofed accounts to imitate senior executives, vendors or customers in order to gain access to corporate IT systems. Historically, BEC attacks focused on the fraudulent transfer of funds, but today they are also used to steal valuable data or to carry out account takeover attacks.

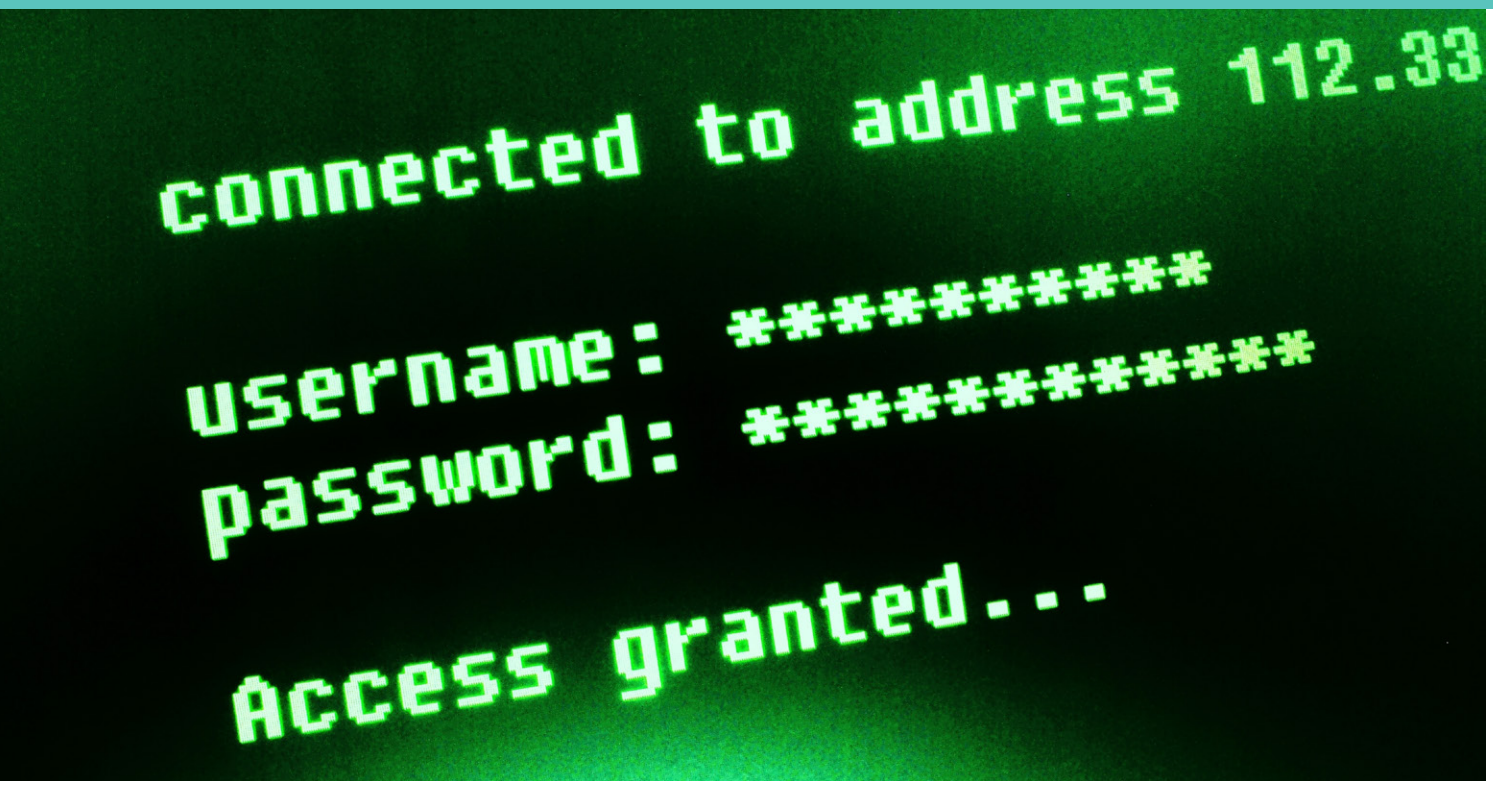
"BEC ATTACKS HAVE GROWN IN SOPHISTICATION"

REMOTE WORKING: CYBER SECURITY CONSIDERATIONS

With many employees around the globe still working remotely, suggested measures to consider for bolstering IT security in the home office include:

- keeping software up-to-date
- activating virus protection and firewalls
- being increasingly cautious about sharing personal data
- making sure web browsers are up-to-date
- keeping passwords safe and changing them regularly
- protecting confidential emails with encryption
- only downloading data from trusted sources
- making regular backups
- turning off voice-activated smart devices and covering webcams when not in use
- making clear distinctions between devices and information for business and personal use and not transferring work between the two
- identifying all participants in online sessions
- logging out when devices are no longer in use and keeping them secure
- following security practices for printing and handling confidential documents
- being careful with suspicious e-mails or attachments

For a full overview of IT security measures, download **Coronavirus: Staying Cyber-Secure Through The Pandemic**



5 MEGA DATA BREACHES COME WITH INCREASING COSTS

Many factors can now contribute to the financial fall-out from such events

The cost of dealing with a large data breach is rising as IT systems and cyber events become more complex, and with the growth in cloud and third-party services. Regulation is also a key factor driving cost, as is growing third-party liability and the prospect of class action litigation.

In particular, so-called mega data breaches (involving more than one million records) are more frequent and expensive. In July 2019, Capital One was hit by one of the largest ever breaches in the banking sector with approximately 100 million customers in the US impacted – more than 30% of the population. This resulted in it being fined $80mn by the US bank regulator. Yet this breach is by no means the largest in recent years.

Data breaches at hotel group Marriott in 2018 and credit score agency Equifax in 2017 were reported to have involved the personal data of over 300 million and 140 million customers respectively. Both companies faced numerous lawsuits and regulatory actions in multiple jurisdictions – the UK's data protection regulator announced its intention to fine Marriott £100mn ($130mn) for the breach. Meanwhile, in the same month – July 2019 – it was announced that British Airways could be fined £183mn ($240mn) for a data breach impacting 500,000 customers in 2018. However, BA ended up paying £20mn ($26mn) – still the largest confirmed penalty issued by the UK's Information Commissioner's Office (ICO) – after the financial impact of Covid-19 was taken into account. It remains to be seen what Marriott will pay.

Nevertheless, a mega breach now costs an average of $50mn[6], according to the Ponemon Institute, an increase of nearly 20% over 2019. For breaches in excess of 50 million records, the cost is estimated to be $392mn, slightly up on 2019.

"REGULATION IS ALSO A KEY FACTOR DRIVING COST, AS IS GROWING THIRD-PARTY LIABILITY AND THE PROSPECT OF CLASS ACTION LITIGATION"

6 IBM Security, Ponemon, Cost Of A Data Breach Report, 2020

6 INCREASING REGULATORY EXPOSURE – AT HOME AND OVERSEAS

Stricter enforcement around increased liability for data breaches and the collection and use of data is to be expected

Data protection and privacy regulation is increasing in both scope and geographical reach, creating more stringent requirements on organizations that collect and use personal data, as well as enhanced rights for consumers and higher penalties for breaches.

In the US, data breach notification requirements have long been an important driver of cyber losses and insurance purchasing – the first such law was introduced in California in 2002, while Alabama became the 50th state to enact a breach notification law in 2018. In recent years, other countries have followed suit – Australia and Canada introduced data breach notification laws in 2018 – while others have gone even further.

Europe's General Data Protection Regulation (GDPR), which came into force in May 2018, has been a game-changer. The law goes far beyond the requirement to notify regulators and individuals of a data breach and significantly raises the bar for consumer rights – it requires companies to gain consent before using data, explain how data is used and erase data when requested. Other jurisdictions have since followed the example of the GDPR and drafted similar laws, most notably California and Brazil, while a number of countries in Asia, Latin America and the Middle East are moving in a similar direction.

This all means that, increasingly, companies need to consider their exposure to regulatory risk, at home and overseas. For example, the GDPR would apply to a US company processing the data of EU citizens, while the California Consumer Privacy Act would apply to a European company holding data on Californians.

The GDPR has already led to an increase in claims notifications. Between March 2019 and May 2020, a total of 190 GDPR fines were issued by European data protection authorities (DPA), according to law firm Pinsent Masons[7]. with a value of almost $500mn. Notable large fines include €50mn ($57mn) for Google in France last year. In September 2020, H&M Germany was fined €35.2mn ($41.3mn) for violations as well.

The landscape has also been complicated further by the July 2020 judgment of the EU Court of Justice in the Schrems II case. This declared that the EU-US Privacy Shield framework is no longer a valid mechanism to transfer personal data from the EU to the US. In response, the US Department of Commerce and the European Commission have initiated discussions for an enhanced framework to comply with the judgment[8].

It all adds up to increased liability for data breaches and the collection and use of data – which goes to the very heart of a modern company – and stricter enforcement is to be expected.

7 Pinsent Masons, EU Data Protection Enforcement Highlights Cyber Focus, October 2020

8 European Commission, Joint Press Statement from European Commissioner for Justice and US Secretary of Commerce, August 10, 2020

7 CLASS ACTION LITIGATION A DEVELOPING SITUATION

Consumers, investors and other stakeholders are increasingly looking to the courts as well if things go wrong

Many large data breaches today spark regulatory actions, but they can also trigger litigation from affected consumers, business partners and investors. When they do, legal expenses can add substantially to the cost.

Data breach litigation in the US is a developing situation. A number of large breaches have triggered class actions by consumers or investors – in July 2019, Equifax reached a $700mn settlement for its 2017 mega breach. US courts have been battling the questions of "legal standing" – whether claimants have the right to sue – but the trend appears to be favoring plaintiffs. Statutory and regulatory changes could also facilitate compensation for data breaches. The **California Consumer Privacy Act**, for example, provides a mechanism for consumers to sue businesses and – in a first for the US – sets statutory damages for data breaches.

Outside the US, a number of countries have expanded group action litigation rights. For example, in Europe, the General Data Protection Regulation (GDPR) makes it easier for victims of a data or privacy breach to seek legal redress.

In addition, claimant law firms and litigation funders are actively looking to bring class actions for data breaches in Europe and elsewhere – a class action against British Airways following its 2018 data breach was given the green light in the UK courts in October 2019. Hotel chain Marriott International is also facing a group action in London on behalf of millions of guests affected by its 2018 breach.

"CLAIMANT LAW FIRMS AND LITIGATION FUNDERS ARE ACTIVELY LOOKING TO BRING CLASS ACTIONS FOR DATA BREACHES"

8 BUYING A COMPANY CAN BRING CYBER RISK

The acquiring firm could still be liable for any damage from incidents which pre-date an M&A

Cyber exposures have emerged as a hot topic in mergers and acquisitions (M&A) following some large data breaches. For example, the 2018 Marriott breach, which has resulted in the international hotel group facing a fine of almost £100mn ($130mn) from regulators, was traced to an intrusion in 2014 at Starwood, a hotel group it acquired in 2016.

Even the best protected companies can be exposed if they acquire a company with weak cyber security or existing vulnerabilities.

Subsequently, the acquiring firm could be liable for any damage from incidents which pre-date the merger.

Ultimately, considering potential cyber vulnerabilities and exposures needs to become a higher priority for businesses during M&A, as many companies are not undertaking enough due diligence in this area. At the same time, once a deal has been completed, many companies do not address any weaknesses in acquired systems quickly enough.

"CONSIDERING POTENTIAL CYBER VULNERABILITIES AND EXPOSURES NEEDS TO BECOME A HIGHER PRIORITY FOR BUSINESSES DURING M&A"

9 NATION STATES INCREASE RISKS

More sponsored attacks causing damage and disruption

The involvement of nation states in cyber-attacks is an increasing risk for companies, which are being targeted for intellectual property or by groups intent on causing disruption or physical damage. Major events like elections and Covid-19 present significant opportunities. During 2020 Google said it has had to block over 11,000 government-sponsored potential cyber-attacks per quarter[9], ranging from phishing campaigns to less common distributed denial of service attacks. Recent years have seen critical infrastructure such as ports and terminals and oil and gas installations hit by cyber-attacks and ransomware campaigns.

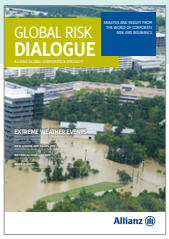
Sophisticated attack techniques and malware may also be filtering down to cyber criminals while nation state involvement is providing increased funding to hackers. Even where companies are not directly targeted, state-backed cyber-attacks can cause collateral damage, as seen with the **NotPetya** malware attack.

9 Google Threat Analysis Group, How We're Tackling Evolving Online Threats, October 2020

RISK MITIGATION:
PREPARE, PRACTICE, PREVENT

Preparation and training are the most effective forms of mitigation and can significantly reduce the likelihood or consequences of a cyber event. Many incidents are the result of human error, which can be mitigated by training, especially in areas like phishing and business email compromise, which are among the most common forms of cyber-attack.

Training could also help mitigate ransomware attacks, although maintaining secure backups can also limit the damage from such incidents. Business resilience and business continuity planning are also key to reducing the impact of a cyber incident, although response plans need to be tested, practiced and regularly reviewed.



↘ Find out more about business continuity plans and desktop exercises

Businesses should consider taking the opportunity to carry out a **desktop exercise** with their insurer and broker, and include key internal and external stakeholders. This builds trust and can take the sting out of any crisis.

Success in mitigating the impact of a cyber event also requires good oversight and knowledge of IT systems and processes across an organization. If there is no overall control or oversight it will take much longer to get on top of a situation. Clear lines of responsibility and communication, and having all departments aligned with an established relationship and master plan, will lead to a more effective response.

The post Covid-19 landscape brings new challenges for businesses. With home-working widespread, security around access points and potential ransomware attacks is critical but organizations should also regularly monitor and ensure there is sufficient network capacity as this can have a significant impact on business income loss if there is an outage. There can also be bandwidth challenges when many employees are video conferencing and companies should ensure they do not compromise availability.

Purchasing cyber insurance should be one of the final points in a company's plan to enhance its cyber resilience. Insurance has a vital role to play in helping companies recover if all other measures are insufficient but it should not replace strategic risk management. Investing in employee awareness, together with updating and continuous monitoring of systems should definitely be at the top of any company's cyber to-do list.

INSURANCE

AGCS has more than a decade of experience in cyber insurance, protecting organizations against cyber-crime and digital threats. It offers a range of cyber insurance products ranging from specialist, standalone cyber insurance to dedicated cyber risk coverage in traditional property and casualty policies.

The types of risks covered include first-party losses (e.g. business interruption, restoration, and crisis communications) and third-party losses, (e.g. data breaches, network interruption, and notification expenses). However, cyber insurance offers much more than just compensation for potentially significant financial losses. AGCS offers valuable prevention and incident response services through its global partner network that helps companies improve their cyber resilience and mitigate negative impacts after an incident. These services include 24/7 access to IT forensic experts or legal or crisis communications support. For more information **https://www.agcs.allianz.com/solutions/financial-lines-insurance/cyber-insurance.html**

About Allianz Global Corporate & Specialty

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 10 dedicated lines of business.

Our customers are as diverse as business can be, ranging from Fortune Global 500 companies to small businesses, and private individuals. Among them are not only the world's largest consumer brands, tech companies and the global aviation and shipping industry, but also wineries, satellite operators or Hollywood film productions. They all look to AGCS for smart answers 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 **32 countries** and through the Allianz Group network and partners in over 200 countries and territories, employing over 4,450 people. As one of the largest Property-Casualty units of Allianz Group, we are backed by strong and stable **financial ratings**. In 2019, AGCS generated a total of €9.1 billion gross premium globally.

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

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

Asia Pacific
Wendy Koh
wendy.koh@allianz.com
+65 6395 3796

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

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

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

North America
Sabrina Glavan
sabrina.glavan@agcs.allianz.com
+1 646 472 1510

UK, Middle East, Nordics
Ailsa Sayers
ailsa.sayers@allianz.com
+44 20 3451 3391

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

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

CREDITS

Editorial: Greg Dobie and Joel Whitehead
Claims Analysis: Daniel Didt and Catalin Toni

Design: Kapusniak Design

For more information contact
agcs.communication@allianz.com

Follow Allianz Global Corporate & Specialty on

Twitter **@AGCS_Insurance** #cyberrisktrends

LinkedIn

For more information on AGCS visit
www.agcs.allianz.com

Allianz Global Corporate & Specialty SE
Königinstr. 28, 80802 Munich, Germany

Photos: Adobe Stock/Shutterstock

October 2020