Cyber Major Loss and Market Update

H1, 2021

Gallagher

Insurance | Risk Management | Consulting

ABOUT GALLAGHER

Founded by Arthur J. Gallagher in Chicago in 1927, Gallagher has grown to be one of the leading insurance brokerage, risk management, and human capital consultant companies in the world. With significant reach internationally, our organisation employs over 32,000 people and our global network provides services in more than 150 countries.

Our people partner with businesses across countries and international territories to provide relevant and impactful professional advice. Regardless of what risk and human capital challenges our clients have, we work hard and utilise industry specific expertise to find the best solution and to deliver it with world-class service. We continue to build on 90 plus years of expertise that spans global industries. No matter the size of the organisation we partner with and the challenges presented by the industry, we work tirelessly to provide solutions that maximise value for our clients.

Our values are core to our culture. Passionate service, strategic innovation, and ethical behaviour form the basis of how we do business. All with one purpose:

TO HELP YOU FACE YOUR FUTURE WITH CONFIDENCE.

Founded in
1927
with headquarters in the US

Listed on the NYSE (AJG)
$24.6bn
Market capitalisation

150+
Countries where we are able to offer client service capabilities

More than
32,000
employees worldwide

Revenues* of
$6bn

3.2%
organic growth rate

850+
offices in 56 countries

2021 WORLD'S MOST ETHICAL COMPANIES® ™
WWW.ETHISPHERE.COM

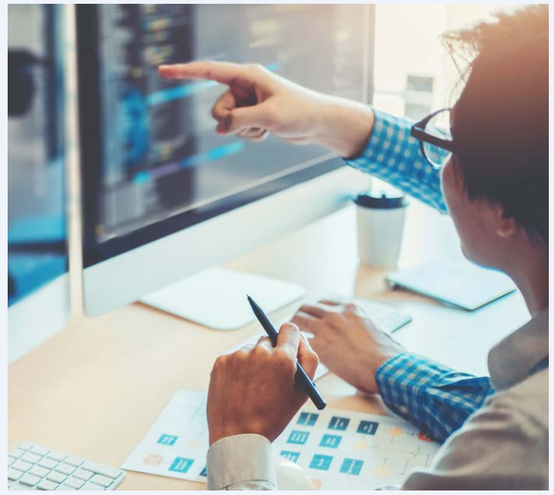
Gallagher has been named one of the World's Most Ethical Companies® for ten straight years. We've been committed to doing the right thing for over 90 years.

All figures correct as at March 2021

**Based on core Brokerage & Risk Management divisions' adjusted revenue for 12 month period*

WHY GALLAGHER FOR CYBER?

Our cyber team has created a number of products to suit a range of industry sectors providing broad cyber coverage, bespoke policy tailoring and consultation.



Our policies cover private data and communications in many different formats – paper, digital or otherwise, and provide 24/7 breach hotlines straight to specialist attorneys.

Who we work with

- Charities/Not for profit
- Construction
- Domestic Services
- E-commerce
- Education
- Financial institutions
- Government
- Healthcare/Medical
- Hotels/Hospitality
- Manufacturing
- Professional services
- Realtors
- Restaurants
- Retail
- Sports clubs/gyms
- Telecoms
- Utilities.

What we offer

- Breach Response Costs
- Cyber Business Interruption
- Cybercrime
- Cyber Extortion
- Cyber Liability
- Cyber Reputation Business
- Income Loss
- Digital Asset Restoration
- Fraud
- Manipulation or Misuse
- Multimedia Liability
- Operational Risk
- Physical Damage (for manufacturers)
- Privacy Regulatory Defence and Penalties
- Security and Privacy Liability.

Contents

01. Introduction

With the rate and capacity changes seen in Q1 2021, we have created a market update to better explain the changes anticipated throughout the rest of Q2.

In this update we provide:

- Cyber insurance market changes in the first half of 2021 and reasons for the change.
- Analysis of ransomware and litigation loss trends.
- Comments on recent major public losses, including those against insurers.
- How Gallagher is assisting clients navigate this changing market.
- Demonstrate our ability to support clients in re-evaluating their cyber exposure with our Cyber Risk Consultants.

We look forward to any questions or any feedback you may have or if there are any themes and topics you would like us to cover in the future.

Tom Draper
Gallagher Cyber Practice Leader

T: +44 (0) 207 204 6223
E: Tom_Draper@ajg.com

02. Gallagher Cyber

A specialist practice supporting clients and Gallagher colleagues across the globe.

- Cyber teams are on the ground in the US, Canada, Australia, Singapore, New Zealand and the UK – over 110 specialists, with a 51 person hub in London covering insurance, risk, claims, underwriting and reinsurance.
- Gallagher Cyber Risk Analytics enables clients to more accurately model their exposures and find the most effective risk transfer solution.
- Our Cyber Risk Consultants enable clients to better identify, quantify and mitigate their exposure, both at a risk and technical security level. This provides our placement teams with a better go to market risk transfer capability.
- Working closely with our sister reinsurance broker, Gallagher Re Cyber, we access limits on behalf of our clients, using global placements in London, Europe, Bermuda, the US and Asia-Pacific.
- We work closely with our Property & Casualty colleagues, as cyber is not a single insurance solution, rather a peril that has a major impact on a client's balance sheet and total insurance portfolio.

03. How 2021 started

Two years of increasing unprofitable cyber books hit a 1/1 cyber treaty reinsurance cycle.

In Q4 2020,

91%

of Gallagher Cyber clients saw a rate increase, with

45% seeing an increase of **20%+**

The 1 January 2021 reinsurance renewals saw the limited cyber reinsurance treaty market look to ensure profitability and reduced systemic issues affecting their books. Nearly

62%

of all cyber insurance premium is ceded to reinsurers – one of the highest of any class.[1] Why? To enable insurers to better protect themselves from a "new" class of business that can have systemic losses.

[1] *Source: https://www.swissre.com/reinsurance/property-and-casualty/reinsurance/casualty-reinsurance-underwriting/cyber-reinsurance-in-the-new-normal.html*

04. Market personnel news in Q1

Beazley's combined ratio deteriorates to 109% on COVID & ransomware[2]

Beazley has reported that its combined ratio deteriorated to 109% in 2020 on the back of first-party COVID-19 losses and elevated ransomware reserves, as the firm announces a loss before tax of USD50.4 million for the year.

Argo exits SME cyber line of business, head of cyber steps down – Inside P&C[3]

Argo Group International Holdings Ltd. exited the small and medium-sized enterprises cyber line of business, Inside P&C reported.

AIG introduces ransomware co-insurance and sub-limits at 1.1 cyber renewals[4]

Market sources said the new measures were introduced at 1 January renewals and that the insurer now requires policyholders to absorb half the cost of digital extortion losses that hit primary and excess policies written below the USD30m mark.

[2] *Source: https://www.reinsurancene.ws/beazleys-combined-ratio-deteriorates-to-109-on-covid-ransomware/#:~:text=Beazley's%20combined%20ratio%20deteriorates%20to%20109%25%20on%20COVID%20%26%20ransomware,-5th%20February%202021&text=Beazley%20has%20reported%20that%20its,%2450.4%20million%20for%20the%20year.*

[3] *Source: https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/argo-exits-sme-cyber-line-of-business-head-of-cyber-steps-down-8211-inside-p-c-59247942#:~:text=30%20Jun%2C%202020-,Argo%20exits%20SME%20cyber%20line%20of%20business%2C%20head,cyber%20steps%20down%20%E2%80%93%20Inside%20P%26C&text=Argo%20Group%20International%20Holdings%20Ltd,company's%20global%20portfolio%20and%20operations.*

[4] *Source: https://www.insuranceinsider.com/article/2876n8ua7o41yv0as0buo/aig-introduces-ransomware-co-insurance-and-sub-limits-at-1-1-cyber-renewals*

05. Key cause of loss: Ransomware

A minor ransomware event three years ago was the No. 1 cause of a cyber event in 2019, 2020 and 2021.

- Negotiated payments range from 10%-65% of demanded amounts, depending on the nature of the variant and the negotiating position of the attacker.
- The biggest costs historically seen with an event are the subsequent mitigation and business impact costs – "downtime costs".
- New variants seen from historic attackers. Conti variant from the same team that deployed Ryuk in 2019-20.[5]

Q4 2019 average ransom demand **$12.8m**

Downtime costs are **5-10 times** ransomware payments

Sanction rules require use of experienced negotiation teams **– Know Your Attacker**

Average number of days a ransomware incident lasts: **21 days**

Q4 2020 average ransom demand **$42m**

Potential logic behind demands? **1% of global revenue**

70% of attacks threaten to **publicise data**

Largest demand seen in H1, 2021 **$65m+**

Decryption can take minutes, but can also **take weeks**

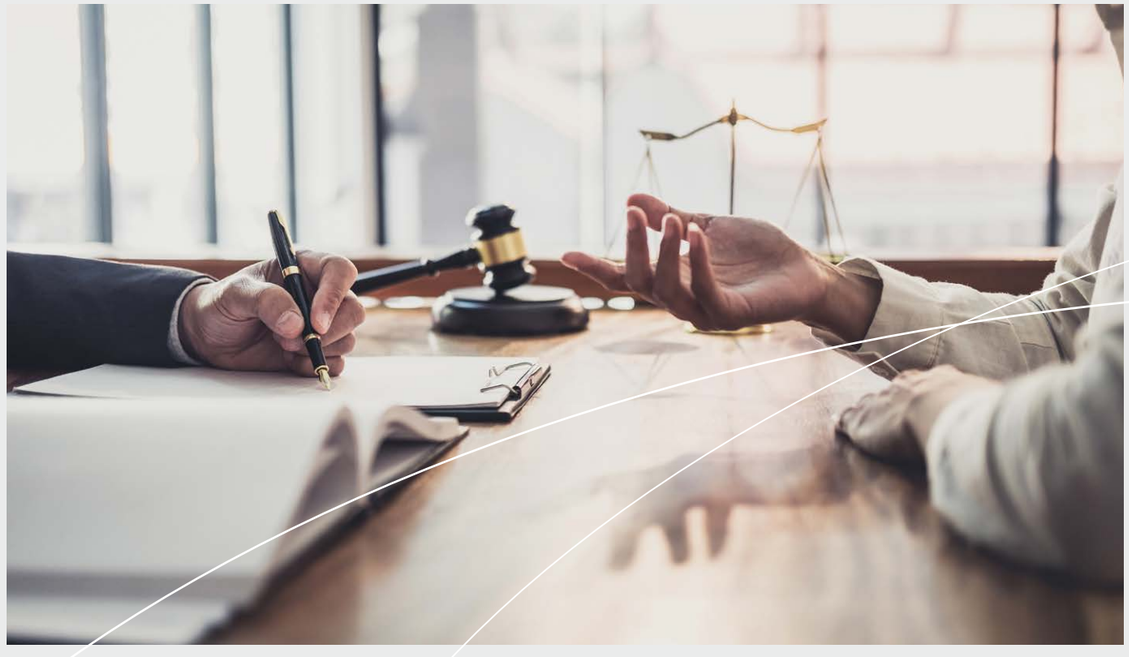
[5] *Source: https://www.areteir.com/is-conti-the-new-ryuk/*

06. Key cause of loss: Litigation

There has been an increase in severity, which has become a key theme in litigation losses, with more laws allowing greater right of action for impacted individuals as well as increasing awards in damages without including legal fees.

- Most recent privacy and security law updates have had a common theme – enabling a far greater right of action for the individual.
- EU GDPR, Illinois BIPA and California CCPA have enabled law firms to prosecute entities on behalf of impacted individuals.[6] This has turned minor issues into major events and major issues into catastrophic concerns.
- UK law firms are able to offer impacted consumers no win no fee, while taking 35% of the final settlement and the downside protected by ATE (After The Event) insurance.
- Average damages for a UK impacted individual for a breach of personal information – GBP2.5k not including legal fees.
- Average damages for a UK impacted individual for breach of healthcare information – GBP8k not including legal fees.
- British Airways class action of 16,000 individuals will potentially cost 2-5 times their penalty from the UK data protection authority.

[6] *Source: Market Knowledge*



07. Recent major losses

Since 2019, 2,103 companies have suffered a ransomware attack that has seen a further release of data.

For example, the perpetrators behind the attacks on Colonial and Brenntag have extorted over USD90m in the past nine months as seen in the chart below:

Entity	Industry	Commentary
Irish National Healthcare System[7]	Healthcare, Ireland	May ransomware attack leading to hospital closures. USD20m demand following theft of 700GB patient data
AXA[8]	Insurance, Asia	3TB personal data stolen in May ransomware and DDoS attack against Asian operations
C.N.A[9]	Insurance, US	March ransomware attack saw 15,000 devices encrypted and systems restored in May after USD40m ransom paid
Colonial[10]	Energy/Pipeline, US	May ransomware attack impacting main fuel pipeline across US SE and NE. USD5m ransom payment made
Brenntag[11]	Chemicals, Germany	May ransomware attack, 150GB data stolen. Demand of USD7.5m, payment of USD4.4m made

[7] *Source: https://www.bbc.co.uk/news/world-europe-57197688*

[8] *Source: https://www.securitymagazine.com/articles/95245-insurance-giant-axa-victim-of-ransomware-attack*

[9] *Source: https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack*

[10] *Source: https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html#:~:text=WASHINGTON%20%E2%80%94%20Colonial%20Pipeline's%20CEO%20told,and%20down%20the%20East%20Coast.&text=%E2%80%9CBy%206%3A10%20A.M.%2C,pipelines%20had%20been%20shut%20down.%E2%80%9D*

[11] *Source: https://www.bleepingcomputer.com/news/security/chemical-distributor-pays-44-million-to-darkside-ransomware/*

08. Market reaction and challenges

How are markets looking to drive their portfolio back to profitability? The markets have replicated what has occurred in the Directors' & Officers' (D&O) market and in other lines, but in a shorter time period, with the main developments as follows:

Increased minimum security standards

Cyber insurers have established increased requirements for coverage to mitigate the probability of cyber events impacting their policyholders. These range from Multi Factor Authentication for remote access, through to increased end-point protection and demonstration of effective back up protections against ransomware attacks.

Rate increases

One of the major legacy cyber insurers has achieved a 191% increase.

Gallagher has not seen such numbers on our large risk book, but risks that saw rate increases of 10-30% in Q1 saw 45%-85% in Q2. Most impacted are XS layers, where minimum premiums have increased to reflect the catastrophic nature of losses.

Retention/Sublimited covers/Line size

While rate can drive profitability, poor security controls have been mitigated by either straight declining accounts or providing higher retention and sublimited covers. AIG[12] led the way with sublimits and coinsurance for ransomware events across all modules, and this has been followed by nearly all cyber insurers. This has also been followed by the average line deployed dropping from USD/GBP10m to USD/GBP5m, with increased focus on quota share by insurers to mitigate their exposure.

Capacity concerns

Cyber insurance, as previously commented, is a heavily reinsured class. The rate increases along with line size reduction has seen insurers hit their premium caps far earlier than expected. We expect most syndicates and global cyber insurers to be effectively closed for new business come September/October, reducing competition for renewing accounts in Q3 and Q4.

[12] *Source: https://www.insuranceinsider.com/article/2876n8ua7o41yv0as0buo/aig-introduces-ransomware-co-insurance-and-sub-limits-at-1-1-cyber-renewals*

09. The Gallagher Cyber solution

How Gallagher can assist to navigate this changing market.

1. Understanding your security maturity / how a cyber event could impact your business

Through our online risk assessment application process called SecureHalo, we can provide your team with a better understanding of the cyber maturity of the organisation and where additional investment will reduce the impact of a cyber event. For many new clients and existing complex ones looking to re-evaluate their cyber risk transfer our cyber risk consultants can engage to provide a workshop, threat assessment and risk mitigation report to drill deeper down into impact of a cyber event on your business, customers and suppliers.

Result: Ensuring the risk and leadership teams fully understand the cyber exposures of the organisation, including monetary impact.

2. Review of timing to approach the market with full information

With the capacity changes and monthly rate movement, a key part of our renewal process is timing the approach to market and ensuring we do so with as much information to drive an optimal result. Gallagher will assist you with identifying this time frame, suggesting extensions where relevant, and how to proactively engage with markets in a COVID-19 world.

Result: Enables insureds to demonstrate to underwriters those investments that in the long term will reduce the probability of a loss and therefore premiums.

3. Reviewing retention structures and quota share placements

Our historic approach with clients to consider cyber as a catastrophic exposure, and to therefore pick a retention driven by cash flow analysis, rather than market sentiment, as been validated by insurer changes. QS Placements have also enabled capacity to be replaced and reduce rate increases – as well as to pay claims quickly. However, each client and program is different, so the team will work with you to ensure the structure is the one most appropriate for the risk.

Result: Providing a cost efficient program, while driving market efficiencies through policy structures.

4. Long term insurer partnerships, but also engagement with new capacity

Gallagher's Cyber practice has established long-term partnerships with syndicates and insurers that have supported our clients through major losses, including complex global claims. With the market changes, Gallagher has engaged with new entrants bringing fresh capacity to the market.

Result: Enabling clients to benefit from experienced insurers who have paid claims and understand complex losses, while also supporting reduction in capacity with new insurers.

10. Cyber risk assessment

We start with a risk workshop led by our cyber risk consultants, who work with clients and the business units to map out the cyber exposures faced, how exposures are mitigated and benchmark that against best practice.

This is supported with a cyber threat assessment that looks at the adversaries, whether human or not, who have the intent and capability to attack your team, data and systems in order to steal intellectual property, personal information or disrupt operations.

The information collected allows us to identify vulnerabilities and risks across the organisation and its digital environment: this is a powerful tool in continuous improvement, management oversight, and insurance placement. We are speaking the language of risk and building off our client's security partners and internal teams – not looking to replace them.

Our final report will incorporate the findings from our overall assessment that is designed to be accessible for senior management: ultimately, giving a broad overview of organisational cyber risk. It will include an overview of the risk workshop, threat assessment, risk identification and risk treatment plan. This will include:

- Our assessment of the current state of play of information security governance and management;
- An understanding of how systems are structured, interconnected, and provide an overview of their levels of resilience;
- An identification of the critical organisational dependencies which might lead to a significant cyber exposure, and a forecast of the likely impacts to the company and its stakeholders;
- An overview of the cyber threat actors that are likely to target the organisation, and the techniques used;
- A suggested risk management roadmap, and reassurance around the areas in which the organisation is already managing risk well;
- An assessment of overall levels of risk, and opportunities for risk transfer into the insurance market including limits and coverage;
- All the information required for an approach to insurers.

The information collected allows us to identify vulnerabilities and risks across the organisation and its digital environment: this is a powerful tool in continuous improvement, management oversight, and insurance placement.

Likelihood

Over a 5-year time period:

THREAT Likely	The chance of this happening is > 50%
THREAT Possible	The chance of this happening is around 50%
THREAT Unlikely	The chance of this happening is < 50%

Impact

A single incident would:

IMPACT High	Potentially result heavy information loss
IMPACT Medium	Result in interruption, or heavy reputational damage
IMPACT Low	Result in financial or other loss

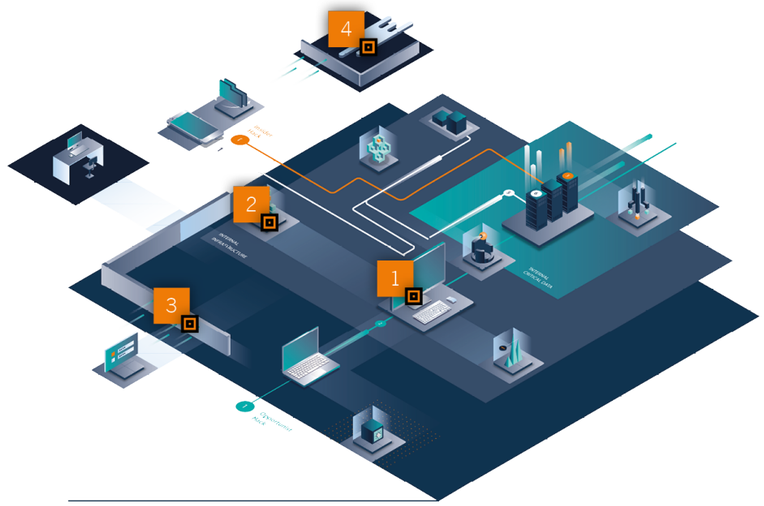
Identified vulnerabilities

1 Vulnerability 1

2 Vulnerability 2

3 Vulnerability 3

4 Vulnerability 4

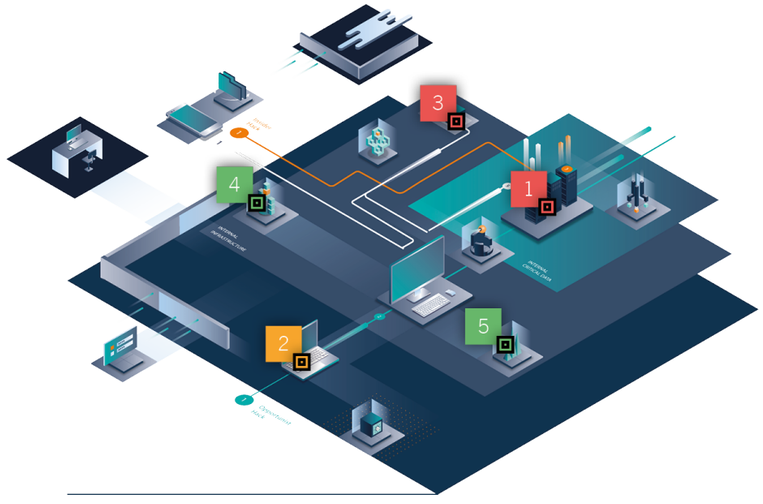


Identified risks

High 2 risks

Medium 1 risk

Low 2 risks



11. Summary

2021 has been a variable time for the cyber insurance market, both in terms of losses and capacity changes.

Clients are seeing substantial changes in a class where they have ever known rate reductions and expansion in coverage. Now more important than ever, it is key for cyber insurance to be part of a holistic approach to risk.

Our team is designed to cater for a client's specific concerns and risk management structures, to provide a more individual service while operating under our clear cyber framework.

We look forward to any questions you may have and if you would like to discuss any of the topics in more detail, please do not hesitate to get in touch.

Tom Draper
Gallagher Cyber Practice Leader

T: +44 (0) 207 204 6223
E: Tom_Draper@ajg.com

GET IN TOUCH

If you would like further information or to discuss your cyber insurance needs in more detail, please contact us today.

T: 0800 612 2278

E: ukenquiries@ajg.com

www.ajg.com/uk/cyber-insurance

Gallagher

Insurance | Risk Management | Consulting