# Aon's Cyber Insurance Snapshot

Helping EMEA organisations better understand
the 2021 risk & insurance challenges

AON
Empower Results®

# Aon's Cyber Insurance Snapshot

## Helping EMEA organisations better understand the 2021 risk & insurance challenges

In 2021, we expect a year of fluid cyber market dynamics. As we help clients navigate a hard market cycle, we recognise the need to be proactive on cyber placements given a more diligent underwriting process, as well as the need to consider coverage options and creative programme structures to help meet risk transfer objectives.

Our goal as we provide a snapshot of the 2021 cyber insurance marketplace is to support EMEA organisations by bringing context to the challenges – both quantitative and qualitative – that insurers are trying to manage, share data on market trends paired with forward-looking guidance offered by cyber insurers, and prepare EMEA organisations as they approach the market in what is likely to be the most challenging year to date in the history of standalone cyber insurance.

Throughout 2020, insurers reached, and in many instances surpassed, a tipping point as loss frequency and severity outpaced improved risk selection and limited rate increases. The change that's been developing since late 2018, and ultimately tipped the scale in 2020, relates to ransomware activity across all revenue segments, but primarily in the middle market space.

### Key 2020 trends include:

**Claim Frequency** - Aon's Cyber Solutions saw a typical cadence of three new cyber matters per business day globally in 2020, up almost 100% from full year 2019, the majority being ransomware event-related.

**Claim Severity** - The average loss severity climbed each quarter of 2020. In many instances, organisations experienced eight-figure ransomware event-related losses. Also, many of those large matters continue to be adjusted over the course of a year, as subsequent business interruption losses are reviewed, and liability claims are litigated.

**Pricing** - While average pricing increased from 2019 to 2020 by 5% - 10%, guidance from almost all insurers has been that those rate adjustments were not enough to compensate for the increase in frequency and severity of losses.

**Risk Selection** - Insurers bolstered supplemental tools throughout 2020. Some insurers are using public-facing scanning resources to search for vulnerabilities that could be subject to cyber threats, and many have introduced new ransomware specific questionnaires. These efforts are focused on improving insured risk controls, as well as improving risk selection for insurers.

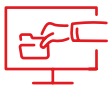
We expect all these trends will continue throughout 2021, at an accelerated pace. Aon's Cyber Solutions has received guidance from some of the largest insurers that we should anticipate 20% - 50% rate increases throughout 2021. To maintain a commitment to long-term, stable cyber capacity, insurers are reviewing areas in the portfolios where underwriting action is needed, and re-evaluating capacity deployment, specifically as it related to ransomware losses.

## Risk Trends to Watch

### Remote Workforce

The remote workforce is here to stay, increasing potential vulnerabilities given Remote Desktop Protocol (RDP) software, remote access security, reliance on third party IT service providers, and digital communication as the primary venue to share information.

### Cyber Extortion



Theft and misuse of personally identifiable information (PII) is no longer the golden goose of bad actors. Ransomware attacks have evolved to include not only the encryption of sensitive data (including PII and confidential corporate information), but also the threat of exposure of sensitive data on the public Internet. These types of attacks may result in corporate downtime due to encrypted networks as well as potential liability consequences in terms of regulatory fines or third-party lawsuits.

### Breach Regulations

The regulatory environment continues to grow in complexity. Recent fines under the European Union General Data Protection Regulation (GDPR) demonstrate that organisations should be mindful of the impact of a breach.Over 160,000 data breach notifications have been reported across the 28 European Union Member States plus Norway, Iceland and Liechtenstein since the GDPR came into force on 25 May 2018. Moreover, GDPR fines rose by nearly 40% in 2020, penalties under the GDPR totalled €158.5 million with the largest fine in 2020 of €35 million issued by the German regulator. Italy's regulator imposed more that €60 million in aggregate GDPR fines. The highest GDPR fine to date remains the €50 million fine imposed by the French regulator.[1] Continued evolution in this space could bring larger financial concerns from a fines and penalties standpoint. The Protection of Personal Information Act (POPIA), came into effect in South Africa on 1 July 2020, to regulate the processing of personal information in harmony with international privacy standards.

### Vendor Risk

As organisations continue to adapt to the current business environment and associated market needs, reliance on third-party technology and back-end applications has never been higher. Supplier cyber security standards are a critical part of this equation. The SolarWinds compromise and the recent Microsoft Exchange vulnerabilities demonstrate the complexity of technology supplier relationships and how they may potentially add risks that may impact cyber security posture.

### Uncovered Technology Professional Indemnity (PI)

COVID-19 has accelerated digital transformation initiatives for many organisations. The emergence of technology services and product exposures in more traditional industries represents a potentially "uncovered" PI exposure that may not be contemplated from liability and financial loss standpoints.

*1 Source: Insights publication research from DLA Piper; https://www.enforcementtracker.com/*

## Cyber Pricing Trends

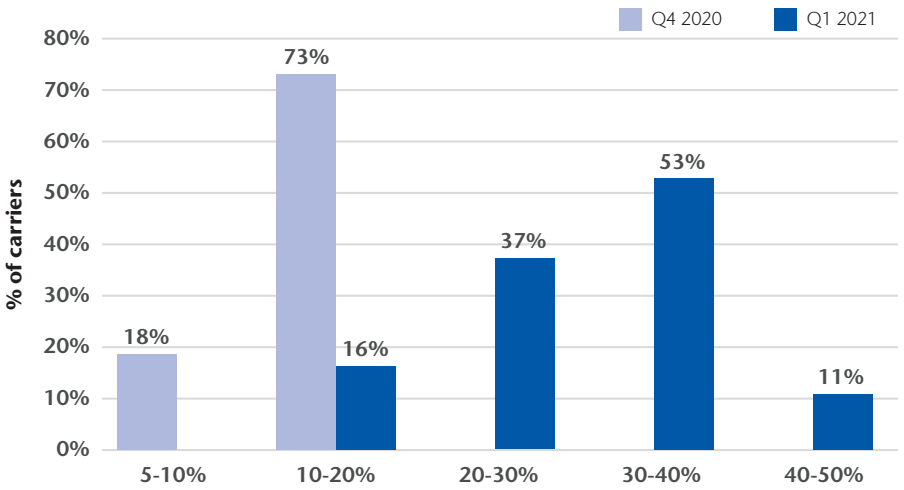
# Results Rate Guidance Changes Across the Entire Portfolio Q4 2020 vs Q1 2021

### Key Commentary:

Aon pricing data is real-time on a historical basis and examines the year-over-year price change on a quarterly basis.

- 2020 Q4 Average rate change from carriers was of **+12%**
- 2021 Q1 Average rate change from carriers was of **+35%** which represents a **23% increase** versus the previous quarter.

However, cyber rates are rapidly changing.




*Guidance is provided through Aon's proprietary survey of the major Cyber insurers Aon trades with. This is not proposed pricing, or guidance specific to a particular insured's programme. This is portfolio level guidance offered by underwriters who participated in the survey.

Source: Aon EMEA Cyber Carrier Survey Q1 2021

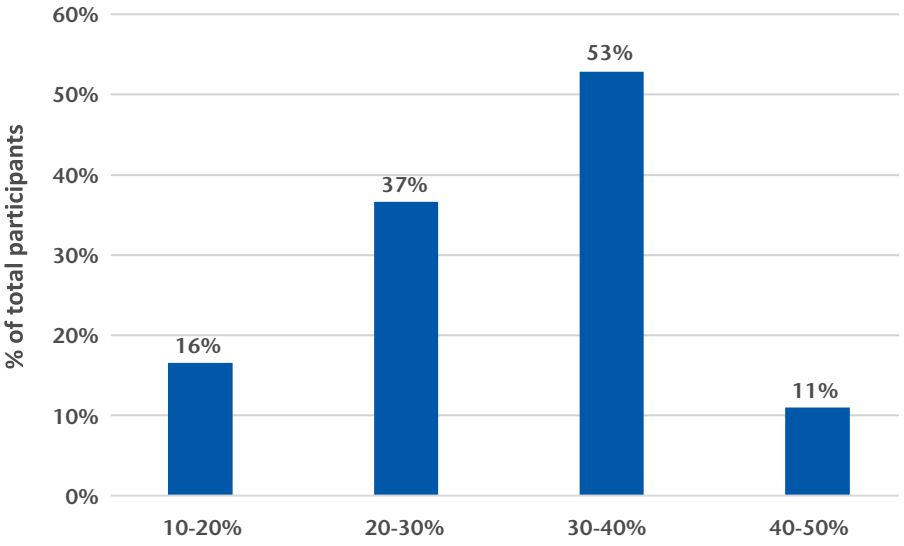
## Forward Looking Guidance

# Rate Guidance Across the Entire Portfolio (Q1 2021)

### Key Commentary:

Aon releases a quarterly survey of the major underwriters in the Cyber space. Below are some key pricing dynamics being felt throughout 2021:

- Majority of respondents suggested they are seeking rate increases **greater than 30% throughout Q2 2021.**
- This information is based on an Insurer's overall rate targets for their portfolio. Each insured has a slightly different risk profile. It's important to represent to insurers how a particular Insured is best prepared to manage its own Cyber risks
- No insurers that responded suggested rate increase would be less than 10% Year on Year going in to Q2 2021
- Aon anticipates pricing to be fluid throughout 2021



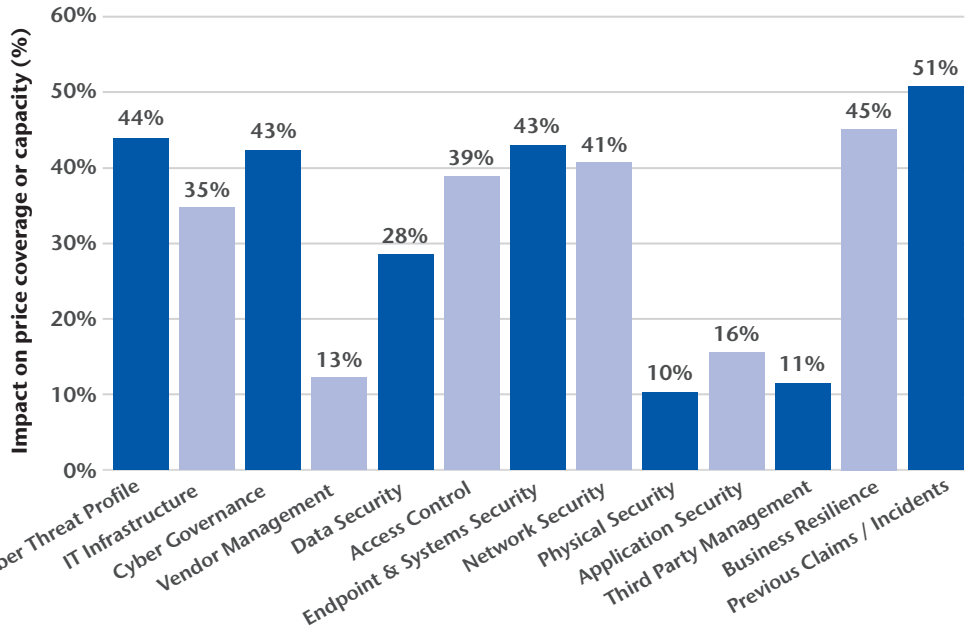

*Guidance is provided through Aon's proprietary survey of the major Cyber insurers Aon trades with. This is not proposed pricing, or guidance specific to a particular insured's programme. This is portfolio level guidance offered by underwriters who participated in the survey.

Source: Aon EMEA Cyber Carrier Survey Q1 2021

# Key Underwriting Topics

## Key Commentary:

- These topics are based on guidance from insurers on a forward-looking basis.
- These topics show the criticality to the underwriting process, however this list is by no means limited to these topics alone and should be considered a starting point for underwriting discussions based on specific industry and individual risk exposures.

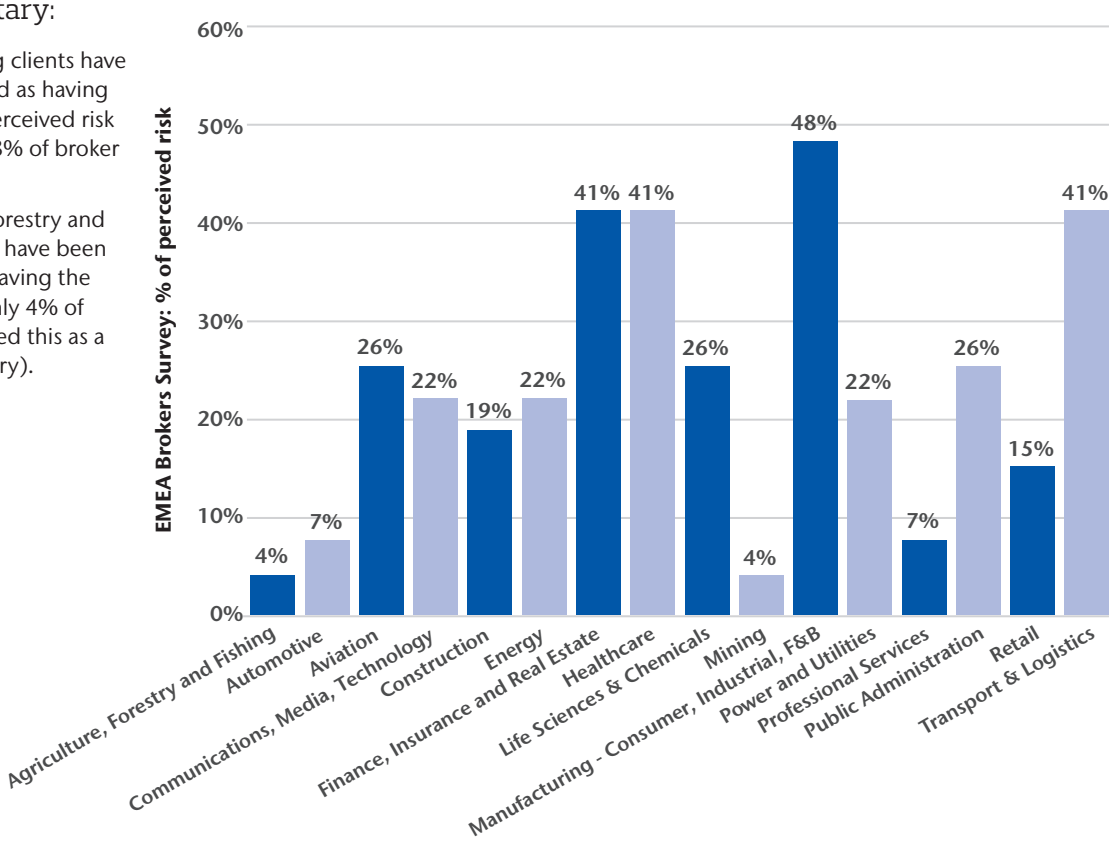



Source: Aon EMEA Cyber Carrier Survey Q1 2021

# Industry Verticals Perceived at Greatest Risk During Q1 2021

## Key Commentary:

- Manufacturing clients have been identified as having the highest perceived risk (elected by 48% of broker respondents).
- Agriculture, Forestry and Fishing clients have been identified as having the lowest risk (only 4% of brokers selected this as a key risk industry).




Source: Aon EMEA Cyber Broker Survey Q1 2021

## Coverage Considerations

In response to the risk and loss trends described previously, insurers are adjusting their underwriting approach, reviewing terms and conditions of coverage, and re-evaluating capacity deployment. The following are specific examples of coverage considerations that insureds will need to navigate in 2021.

### Ransomware Event Coverage


Ransomware events and their associated losses are cited by many insurers as a major factor impacting their cyber insurance loss ratios. Should appropriate underwriting information not be provided, or if the information provided is viewed unfavourably, insurers may seek to limit their coverage for ransomware event losses.

- Several insurers are moving to a limit deployment strategy where they may cap the total aggregate limit they offer to any insured to some factor of the total policy limit. Co-insurance is also being proposed, in some cases, in conjunction with a sub-limit.
- Waiting periods are being reviewed for the business interruption insuring agreements related to ransomware events, again in some cases being as high as 24 hours.
- In the most extreme cases, where critical controls are lacking, insurers may seek to include "ransomware event" exclusions to policies.

It is critical to note that while insurers are using these approaches to limit their exposure, these coverage restrictions are not designed to only apply to a ransomware or cyber extortion insuring agreement. Rather, the restriction is written such that it applies to ransomware as an attack vector (a "ransomware event"), and hence may limit coverage for any loss that would arise from such an attack.

### Dependent Business Interruption

The SolarWinds compromise has caused insurers to review their overall exposure to systemic, aggregated, correlated risks, related to the software supply chain. The breadth of coverage afforded for business interruption losses is being reviewed by several insurers with a specific mind toward limiting the financial exposure to a systemic event in the following ways:

- Reconsidering waiting periods. In many cases, waiting periods had been negotiated to between six and eight hours (and in some instances removed entirely). The marketplace is beginning to push for waiting periods closer to 24 hours, such as those seen in the Property marketplace.
- Limiting aggregate limit exposure. This is being achieved through the reintroduction of sub-limits or requirement of co-insurance.

### Breach Response Vendors

As loss ratios deteriorate, insurers are closely reviewing third-party vendor costs incurred to investigate and respond to cyber incidents. To reduce (or at least combat the increase in) these costs, insurers are demonstrating less flexibility in the use of non-panel or pre-agreed vendors.

In addition to more challenges related to the use of non-panel vendors — particularly if there was no discussion/vetting of the vendor before the vendor's engagement for an incident — insurers are making fewer exceptions related to vendor rates. It is becoming increasingly common for insurers to only reimburse an amount equal to what the insurer would have paid a panel vendor.

## Be a Better Risk – Recommendations

With the shift to a hard cyber insurance market at the close of 2020, a strategic risk based broking approach is critical. Cyber underwriting submission preparation is key to differentiate our EMEA cyber insurance buyers in the market and to maintain access to capital. Beginning the (renewal) placement process early, not only by investing time in the quality of the underwriting submission preparation, but also by meeting with key underwriters, focusing on existing insurer relationships, and determining current (renewal) appetite may mitigate surprises.

### Focus on: Cyber Security

While no organisation can eliminate the threat of a breach, being able to demonstrate basic steps to reduce the risk and significantly decrease the impact of a threat actor is critical. This requires proactive risk mitigation strategies including assessment, testing and practice improvement. It also requires incident response readiness, including conducting table top exercises and proactively retaining key third-party incident response providers. Leveraging resources available through an organisation's insurer partners may improve the outcome should a loss arise. For example, subsequent the recent Microsoft Exchange vulnerabilities, cyber insurers are asking whether organisations are using Microsoft Exchange, and whether they conducted a compromise assessment.

### Focus on: Ransomware & Business Interruption

With insurers seeing both an increase in frequency and severity of ransomware-related losses, companies should be prepared to showcase preparedness for a ransomware attack. Insurers are reviewing this exposure via specific ransomware supplemental questionnaires and use of scanning technology. Focus is on business continuity/disaster recovery planning, privileged access controls, multi-factor authentication, proactive scanning/testing, and overall incident response readiness. This attack vector is of utmost concern to underwriters and will continue to transform the insurance market for next several years.

### Focus on: Privacy

Privacy maturity may be demonstrated via established and updated policies that address third-party contracts, online presence, service providers, supply chains and each business unit. Emerging privacy regulations and requirements should be routinely reviewed with counsel, and insurance language should be reviewed to ensure it is broad enough to meet the evolving environment.

### Focus on: Cyber Security Culture

Employee cyber security and phishing training can demonstrate a culture of cyber security. No longer is this just an Admin/IT/Finance problem, employees should be trained to work to combat malicious actors and reduce common vulnerabilities. Without demonstrating adequate security training, insurers may struggle to provide competitive coverage terms or premium pricing.

### Focus on: Contracts

Third-party contracts are of consideration from a technology supply chain and contingent/dependent business standpoint. Considering the SolarWinds compromise, these critical supply chain and IT vendors are at heightened risk for "single point of failure" hacks impacting multiple organisations. It is critical to understand how both contracts and insurance respond in the case of a supply chain security breach.

### Focus on: Insurer Transparency and Communication

As PI risks grow in complexity, it is important not only to ensure primary insurer engagement relative to coverage terms and conditions, but also to ensure excess insurer understanding of the primary policy provisions. Additionally, it is prudent to review exclusions that could come from other insurance lines such as Crime, Property, Casualty and General Liability. Maintaining a clear and transparent relationship with both primary and excess insurers may better inform policy intent and improve claim outcomes.

# Contacts


**Vanessa Leemans**
Chief Broking Officer
Cyber Solutions EMEA
vanessa.leemans@aon.co.uk

**Alistair Clarke**
Cyber Insurance Leader
Global Broking Centre
alistair.clarke@aon.co.uk

**Naomi Cresswell**
Cyber Insurance Leader
United Kingdom
naomi.cresswell10@aon.co.uk

**Duane Folkard**
Cyber Insurance Leader
United Kingdom
duane.folkard@aon.co.uk

**Søren Carl Stryger**
Cyber Insurance Leader
Nordics
soren.stryger@aon.dk

**Marie-Louise de Smit**
Cyber Insurance Leader
Netherlands
marie-louise.de.smit@aon.nl

**Thomas Pache**
Cyber Insurance Leader
DACH
thomas.pache@aon.de

**Marion Rollandy-Claret**
Cyber Insurance Leader
Switzerland
marion.rollandy-claret@aon.com

**Vincenzo Aliotta**
Cyber Insurance Leader
Italy
Vincenzo.Aliotta@aon.it

**Claudia Beatriz Gomez**
Cyber Insurance Leader
Spain
claudiabeatriz.gomez@aon.es

**Timothee Crespe**
Cyber Insurance Leader
France
timothee.crespe@aon.com

**David Molony**
Cyber Risk Leader
Cyber Solutions EMEA
david.molony@aon.co.uk

**Alex Hornsby**
Senior Cyber Risk Consultant
Cyber Solutions EMEA
alex.hornsby@aon.co.uk

**Karl Curran**
Cyber Insurance Leader
Ireland
Karl.Curran@aon.ie

**Stéfanie Deley**
Cyber Insurance Leader
Belgium
stefanie.deley@aon.com

**Marcos Oliveira**
Cyber Insurance Leader
Portugal
marcos.menezes.oliveira@aon.pt

**John Papageorgiou**
Cyber Insurance Leader
Greece
john.papageorgiou@aon.gr

**Gizem Polat**
Cyber Insurance Leader
Turkey
gizem.guldursun@aon.com.tr

**Eddie Aviad**
Cyber Insurance Leader
Israel
Eddie@aon-israel.com

**Thomas Powell**
Cyber Insurance Leader
Middle East
thomas.powell@aon.ae

**Zamani Ngidi**
Cyber Insurance Leader
South Africa
zamani.ngidi2@aon.co.za

## About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber security, risk and insurance management, investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

## About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance. For further information on our capabilities and to learn how we empower results for clients, please visit : http: //aon.mediaroon.com



**aon.com/cyber-solutions**

AON
Empower Results®