Aon's Cyber Insurance Snapshot

2021 Second Edition, UK and EMEA

Helping organisations make better business decisions
by proactively addressing cyber market challenges

Aon's Cyber Insurance Snapshot

2021 Second Edition, UK and EMEA

Helping organisations make better business decisions by proactively addressing cyber market challenges

In 2021, we have seen volatile cyber market dynamics and expect that the cyber insurance marketplace may become even more challenging as 2021 closes. We anticipate that this will continue into 2022 with the underwriting process maintaining rigour, but with pressure around pricing less severe than what has been experienced in 2021.

Aon's Cyber Solutions has received guidance from some of the largest cyber insurers that we should anticipate 40% - 80% rate increases throughout 2021, and into 2022. It should be noted that insureds in certain industries, with programmes that have been historically priced aggressively, or with deficient underwriting controls, will likely see even greater rate increases.

Our goal is to share loss and pricing trends to date, feedback from insurers, and most importantly, key recommendations for UK and EMEA organisations as we continue to help clients navigate a challenging cyber insurance market cycle.

Aon continues to focus on a strategic, risk-based broking approach. Cyber underwriting submission preparation can be key to differentiate our cyber insurance buyers in the market and to help maintain access to capital. Beginning the (renewal) placement process early, not only by investing time in the quality of the underwriting submission, but also by meeting with key insurers, focusing on existing insurer relationships, and determining current (renewal) appetite, may mitigate surprises.

2021 Cyber Underwriting Trends

During 2021, insurers leaned on five common levers to help determine their perceived best strategy to offer cyber insurance:

1. Focus on pricing discipline

Most insurers have increased rate per million in capital deployment to account for pressure felt across their loss and combined ratios. Aon recorded a typical cadence of three new cyber matters per business day globally throughout 2020 – a near 100% rise from 2019 – while the average loss severity climbed in each quarter of 2020 and, in many cases, became eight figure losses. Ransomware remains the vector attributed to the highest percentage of losses suffered by insurers in 2021.

2. Increase underwriting rigour

All insurers offering cyber insurance have made efforts to improve their underwriting approach, specifically with respect to what insurers perceive to be critical controls to minimize the risk to common ransomware attack methods. Many insurers introduced versions of ransomware supplemental applications in Q1 of 2021. Some insurers have argued that by increasing rigour around risk selection, insureds will also improve their own cyber security posture, creating a healthier ecosystem going forward.

3. Capacity management

Insurers continue to manage capacity deployment across two key fronts. Firstly, they manage aggregation risk by monitoring overall deployment to a single insured, or in common industry sectors. Secondly, many insurers in the first part of 2021 reduced target capacity deployment for any given risk to €5,000,000. For smaller organisations, this change has not caused a significant impact to an insured's ability to obtain adequate coverage. For large organisations purchasing more substantial programmes, the increase in capacity management has created a significant crunch, causing insureds and brokers to develop innovative programme structures to reach aggregate limit goals.

4. Restrictions to coverage

Coverage changes posed by the market were often in combination with capacity management for certain risk issues, specifically ransomware. We saw a small group of insurers introduce sub-limits and co-insurance penalties to all ransomware related losses for insureds perceived to have less than ideal security controls. As we approach the end of 2021, we are seeing certain insurers focus on "systemic risk," with new policy language introduced to help ringfence correlated issues. These changes are tied to insurers' aggregation risk concerns, as threat actors often successfully use critical vendors as a mechanism to enter the environment of dozens, even hundreds, of customers. The rapid scale in which an attack on one vendor can turn into multiple policyholder claims is a challenge some insurers are navigating.

5. Sitting on the sidelines

Some insurers are taking an incredibly conservative approach to cyber insurance. We have seen a small group of insurers exit the segment. Some have narrowed their appetite for cyber risk to a level that limits the product's growth, in turn, limiting the insurance market and an insured's ability to transfer their risk.

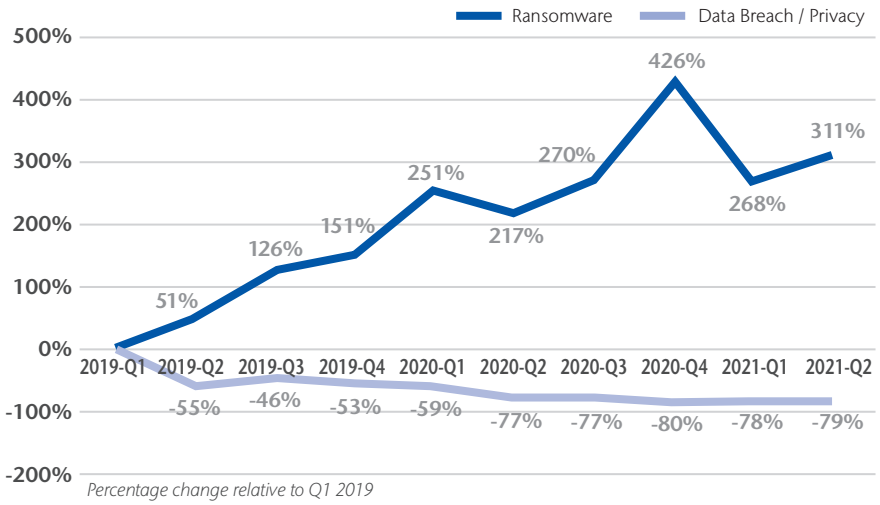
Loss Trends

Frequency of privacy events has continued; however, Aon anticipates the frequency and severity may increase as privacy legislation is tested, and as emerging laws are enacted. Ransomware related incidents continue to be fluid, with the first half of the year's frequency down from Q3 and Q4 2020, while still up compared to the same quarters of prior year.

Cyber Incident Rates Over the Past 9 Quarters

Key Insights:

- Ransomware activity has dramatically outpaced **Data Breach/Privacy Event activity.**
- **Ransomware up 311%** from Q1 2019 to Q2 2021.
- Eight figure losses are commonplace - **business interruption represents the largest component of loss, litigation still to come.**
- Data exfiltration occurred in 77% of ransomware cases per Coveware in Q1 2021.
- Average downtime in Q1 2021, **23 days per Coveware.**

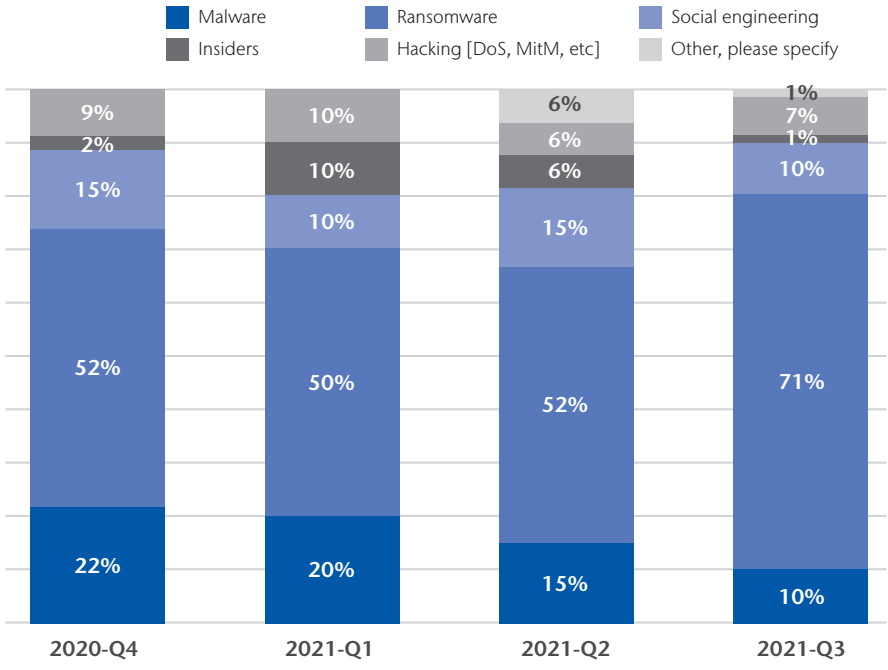


Source: Risk Based Security, analysis by Aon Data as 12/7/2021. Ransomware data exfiltration and downtime per Coveware Quarterly Ransomware Report as of 26/4/2021

Portion of Losses Attributed to Threats & Vulnerabilities, Q4 2020 to Q3 2021 Results

Key Insights:

- This chart illustrates **the attribution of losses to common threat vectors.**
- **Ransomware** remains as the vector attributed to **the highest percentage of losses suffered by insurers.**



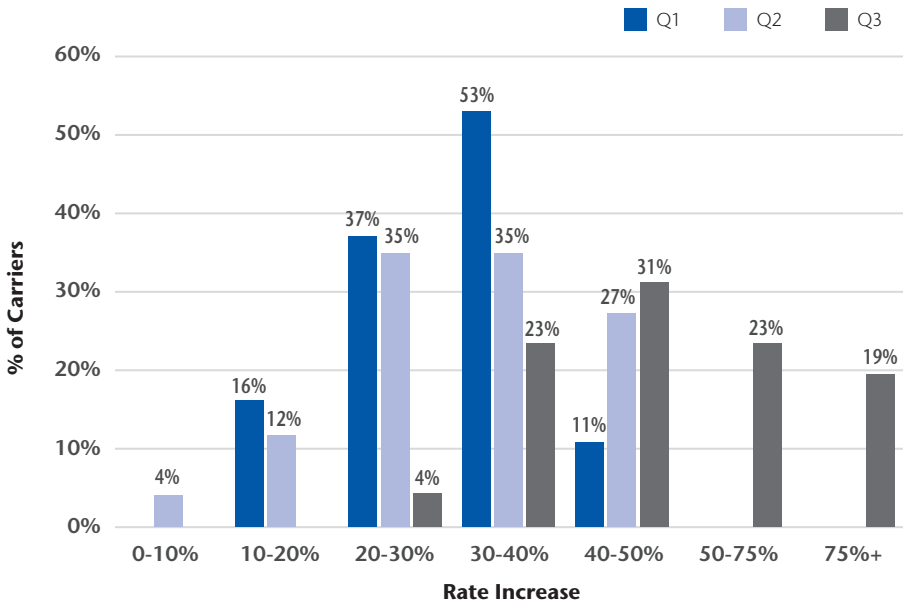
Source: Aon Global Cyber Carrier Survey Q3 2021

Cyber Pricing Trends

Results Rate Guidance Changes Across the Entire Portfolio Q1–Q2–Q3 2021

Key Insights:

- Aon pricing data is real-time on a historical basis and examines the price change on a quarterly basis.
- The average rate increase in EMEA has jumped from **38% in Q2 2021 to 57% in Q3 2021**, with 19% of insurers indicating rate increases higher than 75%.
- While this analysis is meant to highlight trends, we feel it's important to add context that there are industry sectors and client segments which are experiencing far greater disruption to pricing. For example, we've observed many clients in the middle market segment that have seen in excess of 150% rate increases throughout 2021. Insurers continue to stress that rate pressure will not slow down.



*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.

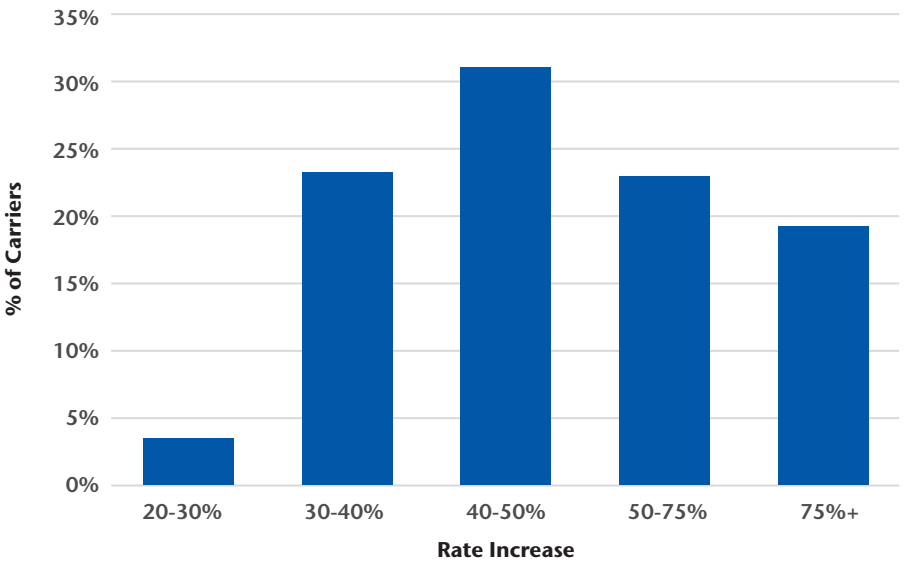
Source: Aon EMEA Cyber Carrier Survey Q3 2021

Looking Forward Guidance

Rate Guidance for the Upcoming Quarter (Q4 2021)

Key Insights:

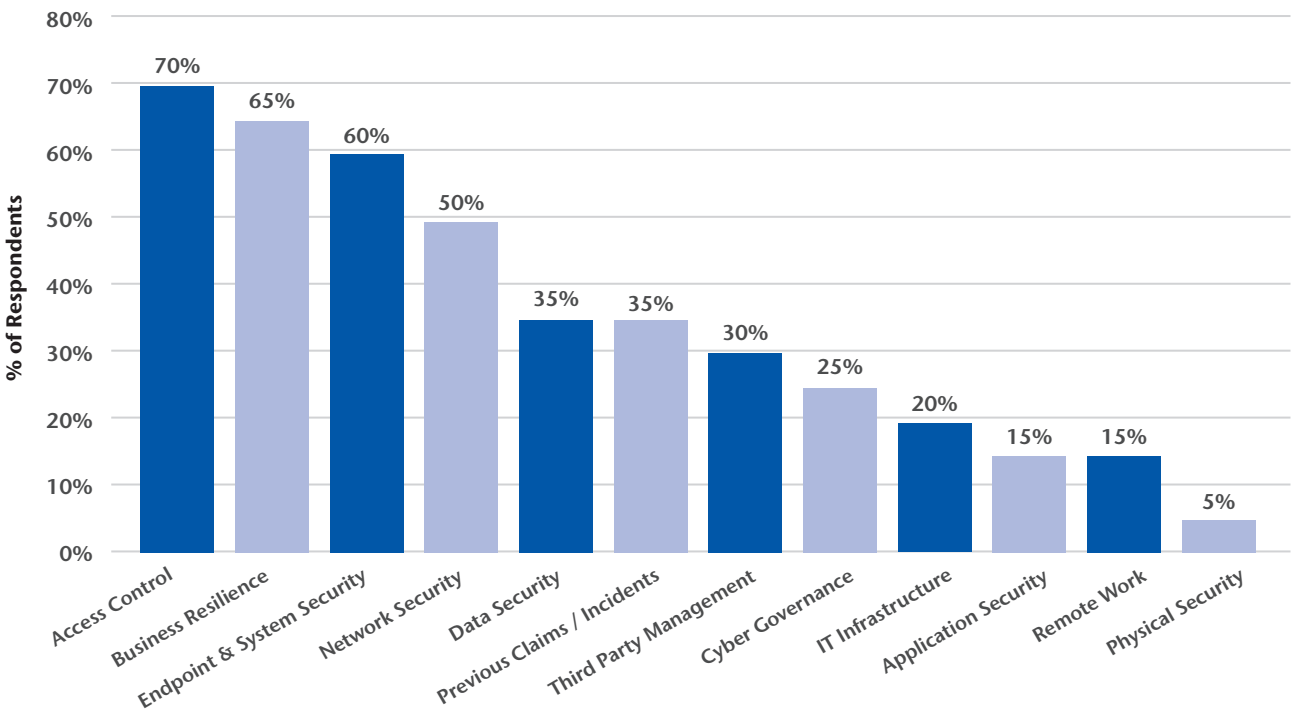
- This chart illustrates the distribution of forward looking rate guidance provided by insurers.
- Insurers continue to stress that rate pressure will not slow down.
- Majority of respondents suggested we should anticipate **40% - 80% rate increases** throughout 2021, and into 2022.



*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 Q3 2021

Key Security Domains Influencing Insurer Declination

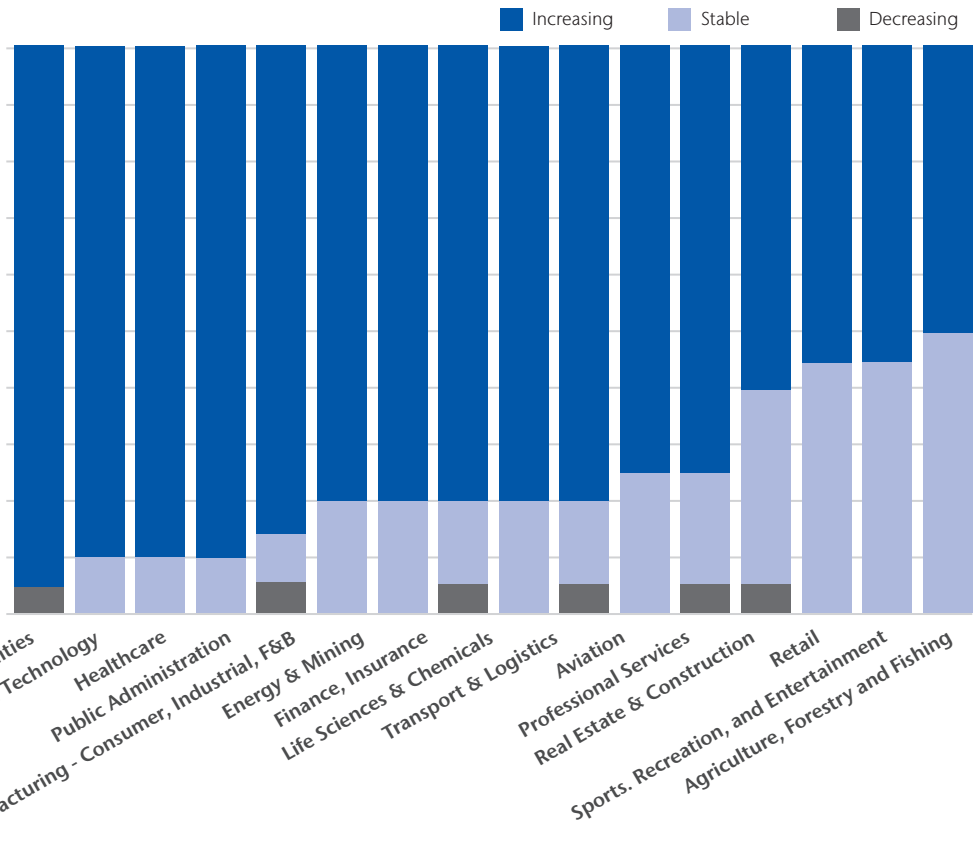


Source: Aon Global Cyber Broker Survey Q3 2021

Industry Risk Outlook

Key Insights:

- This chart illustrates the relative perception of risk across different industry verticals by insurers.
- Insurers have indicated whether organisations in each industry will be facing a heightened, stable, or lessening risk environment.



Source: Aon Global Cyber Carrier Survey Q3 2021

Making Better Business Decisions by Proactively Addressing Hard Market Challenges

In our Cyber Insurance Market Snapshot published in Q2 2021, we outlined key areas where insurers have brought increased attention and scrutiny. Key security domains continue to influence insurer decisions and it is no surprise that adjustment to cyber security strategy, privacy compliance, vendor risk and contractual risk, all remain front and centre across the underwriting community. Aon continues to support clients in preparing robust underwriting submissions to help demonstrate the efforts taken by organisations across each of these key risks and provides salient recommendations as new underwriting concerns emerge.

Organisations need to remain diligent as they enter the marketplace seeking cyber coverage. Beginning the (renewal) process early, in terms of meeting with key insurers, focusing on existing insurer relationships and determining current appetite, may mitigate surprises. Below are some of Aon's recommendations around a strategic, risk-based broking approach to help differentiate your risk in the market:

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 is critical. This requires proactive risk mitigation strategies including assessment, testing and improvement recommendations. It also requires incident response readiness, including conducting tabletop exercises and proactively retaining key third-party incident response providers. Leveraging resources available through an organisation's insurer partners may also help improve the outcome should a loss arise.

Employee cyber security and phishing training can demonstrate a culture of cyber security. No longer is this just an admin, IT or finance problem, employees should be trained to combat malicious actors and reduce common vulnerabilities.

Focus on: Cyber Underwriting Submission Preparation

It's important to start the information gathering process early and to share this with your broker. We help clients to identify pain points insurers will have. In some instances, we can help bolster the context around a particular risk management decision; in others, we can help to improve the cyber security controls. We recommend that clients start the process as early as 150 days prior to the placement date.

In addition, we can support clients through a comprehensive underwriting submission process by presenting a structured and considered approach to cyber security posture.

Focus on: Ransomware & Business Interruption

The topic of ransomware is not going away quickly, if ever. Insurers will continue to focus on key controls that they perceive will limit the probability of a ransomware event, and the severity of the incident. Topics such as lateral movement and business continuity planning in connection to ransomware events will keep developing. Being prepared for this discussion with insurers is critical.

Additionally, we have seen claims friction across two common fronts. Firstly, we continue to see misalignment of vendors or counsel used in response to an event with insurer vendor panels. As policies are put in place, it's important to ensure alignment between insured and insurer on the incident response support that will be used. Secondly, as business interruption and extra expense claims progress through the adjustment process, insureds should have a plan in place to document information needed for cyber business interruption claims, as well as a forensic accounting team with cyber experience, selected to help expedite the proof of loss process.

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 individual business units. Emerging privacy regulations and requirements should be routinely assessed with counsel, and insurance language reviewed to ensure it is broad enough to meet the evolving environment.

Focus on: Supply Chain

Cyber insurers have received a high number of notifications from recent supply chain cyber events, causing them to reconsider how they approach underwriting cyber risks to account for this exposure. Their main concern is the potential for these events to create catastrophic aggregate losses. Examples of supply chain cyber events include Solarwinds and Microsoft Exchange. Insurers are asking organisations specific questions regarding how they have remediated against this exposure. Organisations need to ensure they develop and test cyber incident response and business continuity plans to manage third-party risks.

Focus on: Long-Term Programme Goals

Ten years from now cyber exposures will still pose a material risk to organisations. While a hard market can create tremendous friction and lead to swift decisions around retention or limit, it's important for insureds to develop and maintain a long-term vision of their cyber risk strategy. This view may change the dialogue around certain decisions related to retentions, limits, insurer partners or key coverages for example.

Focus on: Innovation

The most valuable brokers are often those who focus on innovative solutions. It's important for insureds to work closely with their broker, explore various ways to tailor their cyber insurance programme - for example by using the insured's captive - and for the insured to be fully engaged in the submission preparation and placement process.

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

Martin Kainz
Cyber Insurance Leader
Austria
martin.kainz@aon-austria.at

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

Giulio Rosati
Cyber Insurance Leader
Italy
giulio.rosati@aon.it

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

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

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

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) exists to shape decisions for the better — to protect and enrich the lives of people around the world. Our colleagues provide our clients in over 120 countries with advice and solutions that give them the clarity and confidence to make better decisions to protect and grow their business.

aon.com/cyber-solutions