



# NORIMA Risk Forum

16 June 2022





# Agenda

13.30

**Overview and 2022  
Cyber Insurance  
market**

13.45

**Security Controls  
Affecting  
Underwriting &  
Captive Participation**

13.55

**How to navigate the  
market & Best in  
class approach?**

14.10

**Q&A**

# 2022 Cyber Insurance Market

# Businesses Are Facing The Most Challenging Cyber Threat Landscape Yet

With cyber attacks becoming...

## More Frequent

- Global ransomware damage costs are predicted to reach \$20 billion this year, an increase of 57X from 5 years ago
- Ransomware is the fastest growing type of cybercrime and a top cyber threat facing organisations in 2021<sup>1</sup>

## More Targeted

- Attackers are moving away from the “spray and pray” to target practice and big-game hunting
- Targeting victims that can yield a greater financial pay-off<sup>2</sup>

## More Sophisticated

- “Double extortion” attacks
- Taking copies of data and threatening to release it publicly
- Threaten to delete data entirely
- Cold calling victims trying to restore systems<sup>3</sup>

## More Costly

- Some of the most sophisticated ransomware attack groups and malware variants are now averaging over \$780,000 per payment<sup>4</sup>








<sup>1</sup> <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/>

<sup>2</sup> <https://www.wired.co.uk/article/ransomware-trends-2021>

<sup>3</sup> <https://www.itproportal.com/news/ransomware-attacks-set-to-see-huge-growth-in-2021>

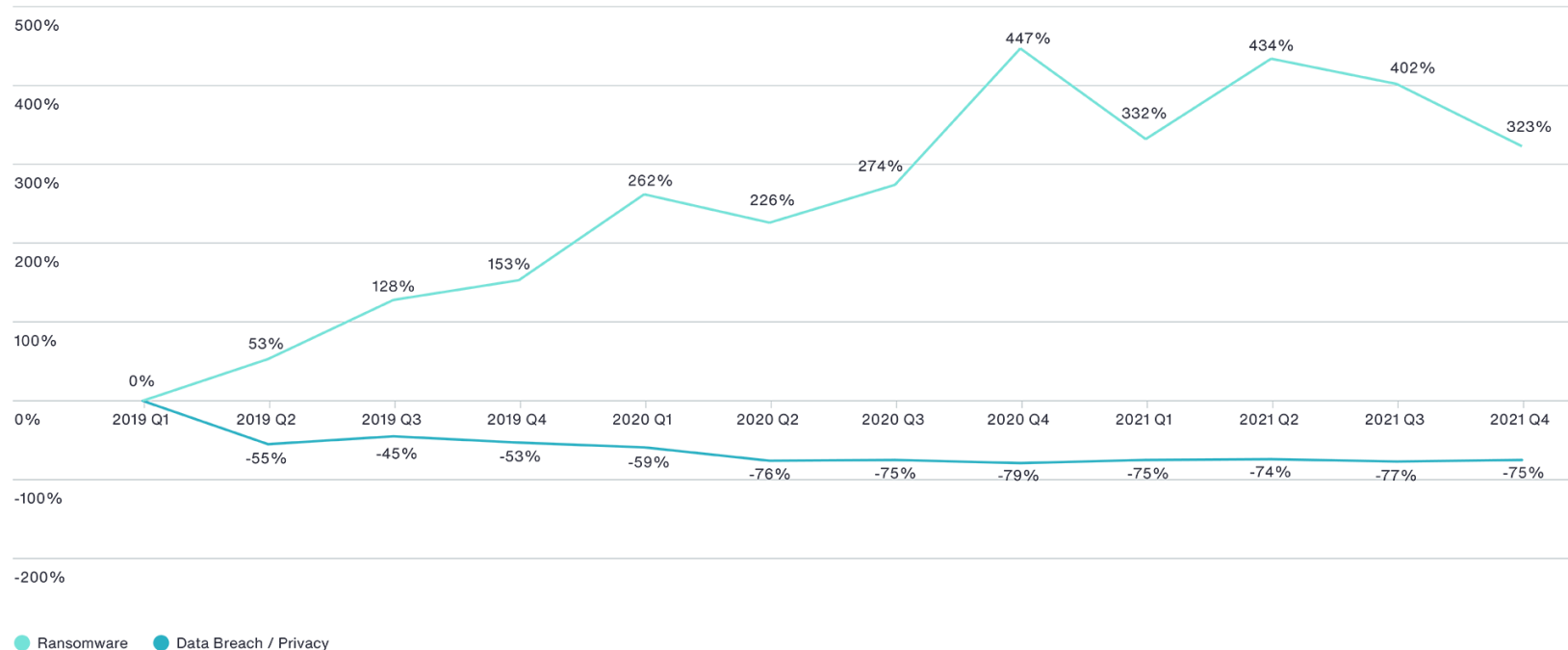
<sup>4</sup> <https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/>

# International Cyber Insurance Market Trends

 <b>Overall</b>	 <b>Coverage</b>	 <b>Limits</b>	 <b>Underwriting</b>	 <b>Capacity</b>	 <b>Pricing</b>	 <b>Deductibles</b>
<p>Markets continue to see material increases in volume and severity of claims</p> <ul style="list-style-type: none"> <li>▪ <b>Ransomware losses</b> continue to proliferate</li> <li>▪ Now also <b>severity losses</b> coming through, affecting traditional XOL markets</li> <li>▪ Complexity of breaches has driven <b>increase incident response expenses</b></li> <li>▪ Markets increase underwriting information. Some insurers are using <b>public-facing cyber vulnerability scanning</b> &amp; many have introduced <b>new ransomware specific questionnaires</b>.</li> </ul>	<p>Coverage overall still broad, but signs of narrowing</p> <ul style="list-style-type: none"> <li>▪ Recent high-profile events underscored concerns <b>systemic</b> potential of cyber</li> <li>▪ Certain markets <b>restrict coverage for ransomware</b> losses, in terms of adding coinsurance and/or sub-limits</li> <li>▪ Broad business interruption coverage available, but can vary across industry class and unique exposures</li> <li>▪ Insurers continue to emphasize <b>panel arrangements</b>, including use of pre-arranged vendors and legal support</li> </ul>	<p>Insurers are imposing coverage restrictions, sub-limits and capacity limitations on ransomware</p> <ul style="list-style-type: none"> <li>• Ransomware sub-limits and co-insurance now commonplace.</li> <li>• Sublimit adjustments are being made for insureds who meet certain underwriting criteria.</li> <li>• On the whole limits remain consistent.</li> </ul>	<p>Underwriting process becoming increasingly rigorous</p> <ul style="list-style-type: none"> <li>▪ Focus on particular control areas with red line and priority items more common place (e.g. Two Factor authentication, IT/OT segmentation etc.)</li> <li>▪ Systemic risk remains the number 1 focus for the market.</li> <li>▪ Outside in portfolio scans are increasingly utilised – results often determining insurability unless explained appropriately.</li> </ul>	<p>Some insurers are reducing capacity</p> <ul style="list-style-type: none"> <li>▪ Insurers are <b>reducing capacity</b> to \$15M / \$10M and evaluating attachment points, may limit capacity further based on segment (middle market average line \$5M) or lack of security controls</li> </ul>	<p>Cyber market conditions are firming, due to ransomware activity</p> <ul style="list-style-type: none"> <li>▪ Average cyber premium increase Aon Cyber Carrier &amp; Broker Survey EMEA : <b>57%</b></li> <li>▪ Some insurers indicating rate increases higher than <b>75% and for major accounts in heavily affected industries over 100%</b>.</li> </ul>	<p>Deductibles are increasing as markets expect insureds to review historical levels</p> <ul style="list-style-type: none"> <li>▪ Retentions of all levels are available in the market, but can vary greatly based on industry class, size and unique exposures</li> <li>▪ Risks with loss activity are likely to see retention increases</li> <li>▪ Captive participation increasingly seen at a deductible buy down layer</li> </ul>

# Loss Trends

Throughout 2021 Aon's team observed a slight reduction in the frequency of cyber claims, although they have risen dramatically since 2018. Severity increased slightly on all fronts, with more material cyber claims in the market than prior years.



## Key observations

- Ransomware activity has dramatically outpaced Data Breach/Privacy Event activity.
- Ransomware up 323% from Q1 2019 to Q4 2021.
- Eight figure losses are commonplace – business interruption represents the largest component of loss, litigation still to come.
- Data exfiltration occurred in 83% of ransomware cases per Coveware in Q3 2021.
- Average days of business interruption in Q3 2021 was 22 days, according to Coveware

# Which Core Market Themes Do We Anticipate Throughout 2022?

## Climbing Rate Environment

- The majority of carriers are signalling significant rate increases for the first half of 2022. We expect this to be comparable to the second half of 2021, but anticipate potential stabilization in the second half of 2022.

## Increased Underwriting Rigor

- We anticipate all insurers offering cyber insurance to continue to bring new scrutiny, applications and underwriting questions into the placement process.
- Insurers will continue to focus on “real time” issues related to new attack methods or emerging tactics and threat actors' leverage to exploit emerging vulnerabilities

## Client Segment Differentiation

- Industries with decentralized security strategies, and those that tend to have heavy merger and acquisition growth strategies, continue to show increased loss activity compared to other industries. Consistently aligning security controls can be difficult for companies in these verticals
- Smaller organizations may experience more rigid positions from underwriters with respect to specific security controls perceived to be critical when protecting against certain attack methods

## Aggregation Risk

- Throughout 2021, many insurers focused on capacity deployment on a risk-by-risk basis, but as 2022 develops, we anticipate many insurers will shift focus to systemic and correlated risk concerns and their impact on the insurer
- Supply chain attack strategies and geopolitical tensions, paired with the reliance many companies have on common technology service providers, will likely drive a focus on war exclusions and infrastructure language in cyber policies.

# Coverage Considerations

Several insurers are reviewing the **breadth of coverage afforded for BI losses** with a specific mind toward limiting their financial exposure to a systemic event by:

- **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, achieved through the **reintroduction of sub-limits** or requirement of coinsurance.

Many insurers are demonstrating less flexibility in using non-panel or pre-agreed **third-party vendors** and making fewer exceptions related to vendor rates. It is becoming increasingly common for insurers only to reimburse an amount equal to what the insurer would have paid a panel vendor.

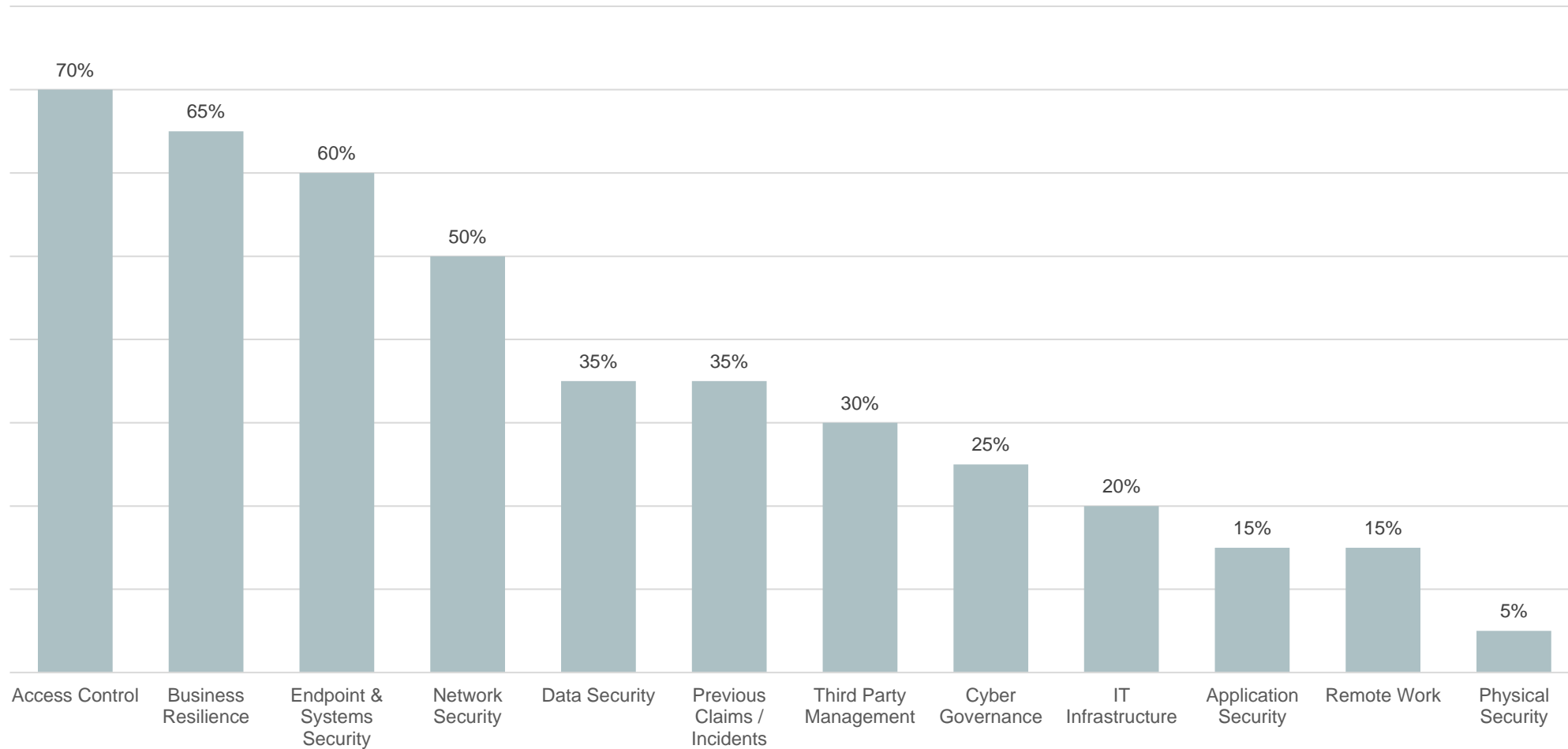
There have not been uniform **war exclusions in cyber policies** to date, we continue to monitor whether any changes are forthcoming and whether any such changes result in a more fragmented approach to war exclusions.



How security controls affect underwriting?

# Key Security Domains Influencing Carrier Declination

## Global



# Captives & Risk Financing

# Cyber Captive Utilization

The majority of organizations are unable to purchase coverage to correspond to their exposures due to a scarcity of capacity and/or prohibitive pricing. Using a captive to provide coverage for the shortfall in full may place unrealistic capital expectations on the captive and so the majority of organizations opt for one or a combination of the three options;

## 1 Deductible infill

Rationale:

- Increasing the deductible and the insurance market attachment point can provide more lead insurer options
- Increasing the deductible can shield the market for smaller notifications, resulting in a more stable partnership with insurers

## 2 Programme gap infill

Rationale:

- Available captive capacity is used to ensure the programme is fulfilled by filling gaps in eth programme. Where there is a deficit of insurance capacity / appetite on a particular layer, the captive can be used as a substitute, enabling the layer to be completed and opening up excess layer capacity.

## 3 No Insurance

Rationale:

- Where an organisation decides against the purchase of insurance due to excessive cost, a captive can be used to evidence insurance where necessary.
- Creating insurance reserves and prefunding the risk on the captive balance sheet may be a more efficient way to finance the risk compared to financing from the group balance sheet.

How to navigate the current market?



# Staying Ahead of the Market

## 1 FOCUS ON: Preparing a Collaborative Underwriting Submission, early....

- Collaborate with your broker during the information gathering stage. While the underwriting requirements from 2021 provide a relevant base for 2022 renewals, the required details and applications have evolved. Gathering the appropriate information and completing the current versions of applications can help prevent a “stale” submission which often delays the process.
- Brokers can also help identify pain points underwriters may have based on preliminary responses. In some instances, it may be possible to bolster the context around a particular risk management decision; in others, it may be possible to help clients explore ways to improve control. Without time, it will not be possible to improve the perceived risk posture before a policy expiration or renewal date. We recommend clients start the process as early as 150 days prior to the placement date.

## 2 FOCUS ON: Long Term Program Goals

- Ten years from now, cyber exposures will likely still pose material risk to companies. We believe companies will continue to buy more insurance, transferring a portion of their risk to insurers. A hard market can create tremendous friction, leading to swift decisions around retention or limit.
- It's important for clients to develop and maintain a long-term vision and manage their insurance program strategy based on those goals. This view may change the dialogue around certain decisions related to retentions, limit, insurer partners and key coverage debates.

# Staying Ahead of the Market

## 3 FOCUS ON: Ransomware and Business Interruption

The topic of ransomware isn't going away quickly, if ever. Insurers will continue to focus on key controls they perceive will limit the probability of a ransomware event and the severity of the event. Topics such as access control, business continuity planning, and patch management remain relevant and will continue to develop. Being prepared for that discussion with underwriters is key.

**Additionally, we've seen claims friction across two common fronts:**

1. **First**, we continue to see misalignment of vendors or counsel used in response to an event, with insurer vendor panels. At least annually (and more often as incident response playbooks are revised) the client's preferred incident response vendors should be discussed in the context of the insurance policy to ensure alignment with the insurers' requirements for pre-approval and/or panel usage.
2. **Second**, as business interruption and extra expense claims progress through the adjustment process, clients should have a plan in place to document information needed for cyber business interruption claims and should have a forensic accounting team – with cyber expertise - selected to help expedite the proof of loss process and maximize the potential recovery.

## 4 FOCUS ON: Creativity

- The most valuable brokers are the ones who are the most creative. We know the market will continue to be challenging; it's important for clients to work closely with their broker, think about various ways to develop an optimal program, and for the insured to be a part of the process.

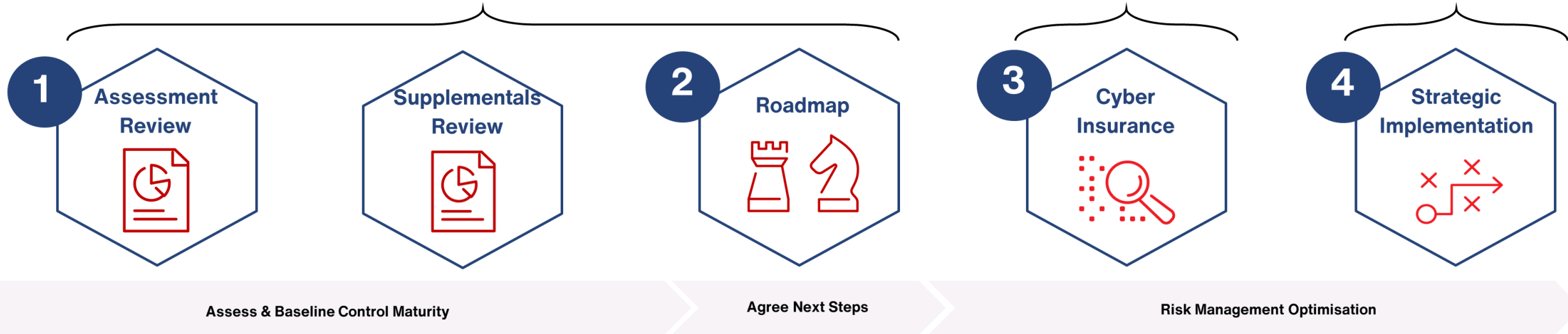
Best in class approach?

# Suggested route to market..

Insurability Readiness Assessment (in-scope)

Risk Transfer

Control Improvement



- ▶ Review of underwriting submission / reports provided to market
- ▶ Presentation of red & yellow flag review of controls based on information provided
- ▶ Deep-dives on areas of underwriter priority, e.g. 2FA, BCM, Back-up and vulnerability management

- ▶ Review of applicable Operational Technology (OT) security assessment supplementals
- ▶ Review of Market-mandated Ransomware supplemental

- ▶ Tailored recommendations on insurance strategy, risk management and security controls
- ▶ Prioritised ISMS roadmap based on agreed findings

- ▶ Agree insurance coverage and programme structure
- ▶ Prepare Cyber Underwriting Material (having conducted Steps 1 & 2)
- ▶ Underwriting presentation and insurer Q&A
- ▶ Receipt of offers and tender / placement activities

- ▶ Partial or full implementation of the recommended risk reduction programme
- ▶ Focus on biggest Return on Security Investment, where possible leveraging existing investments, tooling and teams

# Thank You



**David Molony**  
Head of Cyber EMEA  
[david.molony@aon.com](mailto:david.molony@aon.com)  
<https://www.linkedin.com/in/davidmolony>