Ensuring a future-proof Cyber Insurance Market

Taiwan Annual Insurance Conference

18th October 2022

Munich RE

Agenda議程

Munich RE

- Munich Re's Cyber Proposition & Global Cyber Market 慕再對資安險的展望與國際市場分析
- Cyber as a dynamic threat 資安是一項動態風險
- Accumulation is a serious consideration in writing such a global line of business風險累積不容忽視
- Systemic risks such as war must be avoided to ensure sustainability 系統風險(如戰爭風險)須避免

Dedicated Cyber Resources for the Asian region with global expertise supported by strong local team慕再完整的專家團隊

Munich RE

Belhassen Tonat
General Manager Non-Life
Munich Re Beijing Branch

Professional Affiliations:
- Alumni – LMU Munich (Germany),
- Paris Dauphine University (France),
- ENAss (France),
- INSTEAD (France)

Serene Chan, ACII (LLB Hons)
Head of Cyber Asia
Singapore

Education
- Bachelor of Laws (LLB Hons) King's College London
- Barrister-at-Law, Lincoln's Inn, England

Professional Background
- Regional Senior Cyber UW (4 years) – MR
- Cyber & Intellectual Property Underwriter (6 years) – Tokio Marine Kiln London

Kay/ Kevin
Non-Life representative
Munich Re Taipei

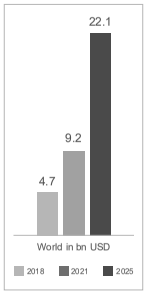
Harprit Singh Narang
Regional Risk Specialist Cyber
Singapore

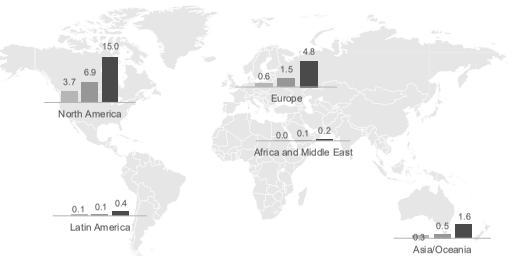
Christopher
Regional Assistant Underwriter Cyber
Singapore

Cyber insurance market with strong expected growth

Munich RE

Worldwide cyber premium: ~USD 5bn (2018) to ~USD 22bn (2025)





Source: Munich Re estimates

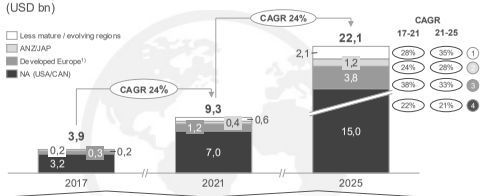
Cyber insurance market with strong expected growth

North America remaining largest market; Europe with strongest growth

資安險具高度成長潛力-北美是最大市場/歐洲具最高成長率

Munich RE

Development of Global GWP
(USD bn)



Coverage widened; rates slowly declined
- A lot of capacity and new markets came into the LoB across all segments
- Especially **AIG, Chubb and Beazley** provided a lot of primary **capacity in many markets** (including immature markets)

Hard market expected until at least 2023
- **Increased number of losses** mostly from ransomware, BI, forensics, data breach
- A number of **carriers pulled out** or reduced **capacity** significantly
- Strong growth expected based on persistent hard market (**rate increases**)

Source: Munich Re
1) U.K, GER, FRA, ESP, ITL, NL, SWE, DK, CH

1 **Less mature regions** – Asia LATAM and evolving European markets – to **remain small** coming from a very low base and given slower take-up than expected previously

2 **ANZ and Japan** growth lower than Europe – so far less impacted by ransomware losses

3 **Developed Europe**[1)] expected to grow significantly faster than US based on **increasing market penetration (exposure)**

4 **North America** still to be source of **two thirds of global business** in 2025 – strong rate increases following ransomware losses

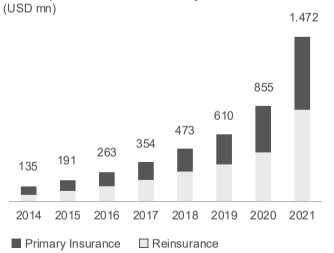
Cyber insurance market with strong expected growth

Cyber is one of Munich Re's main strategic areas

資安險是慕再策略成長業務

Munich RE

Development of Munich Re Cyber GWP
(USD mn)



- Munich Re as **reliable reinsurance partner** for cyber solutions worldwide – active in cyber from the beginning
- **Strong investments into cyber expertise** in the last 8+ years, incl.
  - 100+ underwriting and IT security experts globally
  - Underwriting tools and processes, as well as own accumulation models
- **Strong partnerships within the cyber ecosystem** (accumulation models, IT security startups)
- **Munich Re primary insurance** operations mostly with focus on US and Europe

Source: Munich Re

Munich Re are a leading provider of cyber insurance solutions

慕再居全球資安險領導地位

Munich RE

Cyber insurance is fundamental to economies and successful digitalization

資安險對經濟發展至關重要亦是數位化的致勝關鍵

Sustainable Capacity 提供穩定的承保能量
- Continuing to offer adequate risk transfer solutions by promoting resilience to foster long-term profitability
- Combining adequate cybersecurity standards with appropriate premium and adequate retention levels
- Clearly defined risk appetite while being disciplined in underwriting and stringent in risk management
- Increasing certainty by ensuring clarity of wording and transparency

Cyber Expertise 具備資安險所需專業
- Utilizing the benefits from our early commitment to the cyber challenge and growth opportunity
- Early and continuous investment in multidisciplinary cyber teams with in-depth expertise and a specific focus on accumulation
- Managing the continuously evolving risk landscape in an all-encompassing state-of-the-art manner
- Closely collaborating with clients to understand exposures, their needs and learn firsthand from their experiences

Facilitating a sustainable and profitable cyber insurance market together with our clients

Systemic Risk 監控及管理系統風險
- Tackling the core challenges of cyber exposure to clearly define risks and limits of insurability
- Appropriate mechanisms to make systemic risks explicit and to control exposure
- Consistent coverage for defined exposures while identifying that there are limits of insurability such as infrastructure failure and cyber war
- Engaging in regular exchanges with our clients and model vendors on cyber accumulation issues to properly manage cyber risks
- Ensuring state-of-the-art and fit for purpose accumulation modelling

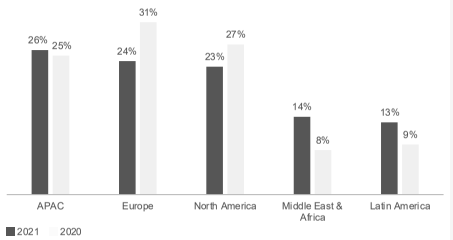
Data 強化資安險相關數據分析管理運用
- Increasing quality and quantity of data on exposures, wording topics, trends and losses
- Reflecting that an understanding of the data provides the basis for risk understanding, underwriting and portfolio steering
- Further investing in partnerships
- Teaming up with clients to share challenges, data and learnings regarding the underlying risks
- Jointly developing innovative data-centric solutions

APAC was the most attacked region in 2021

亞太地區在2021 年遭受最多資安攻擊事件

Munich RE

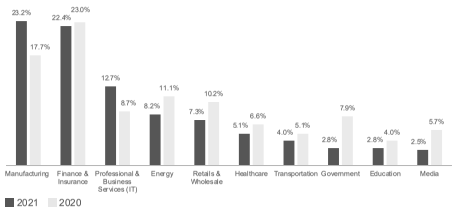
Overview of Global Cyber Attacks by Region
各地區資安攻擊件數一覽表



Deep-dive into attacks on APAC
- **Japan, Australia and India** were most attacked countries within the APAC region
- **Japan** in particular suffered most attacks in the run up and throughout the Tokyo Olympics period
- **Top Types of Attack:** Server access, Ransomware and Data theft, Remote access, were top attack types
- **Top Attack Vectors:** Vulnerability exploitation and Phishing were top attack vectors identified
- **Top impacted industries:** Finance & Insurance, Manufacturing and Business & Professional services were most attacked organizations

Manufacturing & IT Industry most impacted industries due to Supply Chain Attacks
製造業及科技業因供應鍊遭受資安攻擊所受的衝擊最大

Munich RE



- Increase in attacks on **Manufacturers** is largely due to IT complexity, wherein attackers took advantage of the legacy systems and lack of network segmentation setup for widespread scenarios
- **Energy sector**, another industry with OT exposure was targeted along with Manufacturing. This trend will likely continue in 2022

Top Cyber Threats前五大資安攻擊型態

Munich RE

Ransomware網路勒索 (Current Trends: RaaS; Double/Triple Extortions)	1
Phishing網路釣魚 (Current Trends: Theme based patterns, e.g.,: Cryptocurrency related)	2
Supply Chain Attack供應鏈資安攻擊 (Current Trends: SMEs to experience a attack, even if they are not the end target)	3
Cloud Threats雲攻擊 (Current Trends: Hybrid and multi-cloud attacks; exploiting vulnerabilities from mis-config)	4
BEC商務電子郵件被駭 (Current Trends: Shift from CEO frauds to members of executive team or finance dept.; Focus on geo where MFA is not widely implemented)	5

- Rise of **ransomware-as-a-Service groups** and trends like double extortion and Initial Access Brokers becoming the modus operandi to franchise Ransomware attacks
- **Phishing and Social Engineering** remain primary threat vectors with evolving trends
- **Supply Chain attacks** is rising and expected to rise further as organizations are increasingly dependent on highly-interconnected supply chains
- **Cloud adoption** accelerated during the pandemic will lead to security gaps in deployment resulting in attack vector for initial infiltration

Ransomware attacks are evolving rapidly
網路勒索型態日新月異

Munich RE

Ransomware Trends to be aware of

Trends	In the past	Evolution
Extortion Style 勒索樣態	Encryption 加密	Exfiltration (Double/Triple extortion) 數據洩露
Threat actor approach 攻擊方式	Sharing Decryption keys 提供加密鑰匙	Exfiltrated data has ended up online even after payment付贖款後仍可能被洩露數據
Big Game Hunting 打怪目的	What they can get 想獲得特定利益	Access to entire network 想進入整個被駭者的網絡
RDP compromise 遠距桌面協議被駭	Phishing 網路釣魚	RDP Comprise & software vulnerability exploitation 網絡漏洞利用
Supply Chain Attack 供應鏈攻擊	Single Victim 單一受害者	Blast Radius 衝擊廣泛

Cyber as a new man-made peril
資安視為新的人為的事故

Munich RE

- Cyber risk has only emerged as a peril in recent years
- Series of "prominent" incidents in the recent past
- Attacks are driven by human behavior rather than by natural forces
- Attack capabilities improve steadily by increased efforts of threat actors also in response to amendments in defences
- Increasing loss potential as reliance on digital technologies increases
- Changing legal and regulatory environment (e.g., GDPR) leads to changes in financial implications

Dyn DDoS Attack

Accumulation Potential & Loss Events
風險累積及損失事件

Munich RE

Observed Accumulation Paths

- Common software vulnerability (Wannacry, NotPetya)
- Common hardware vulnerability (Meltdown, Spectre)
- Disruptions to IT Service Providers (Amazon S3 Outage)
- Attacks on critical infrastructure and/or industrial control systems

Ransomware worm: NotPetya

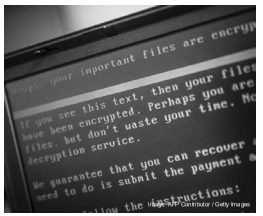


Image: Future Contributor / Getty Images

Significant Accumulation Potential arises form shared vulnerabilities and disruption/outage of central IT services and external networks

Cyber risk Management approach at Munich Re
慕再資安風險管理方法

Munich RE

Risk management approach 風險管理方法:

Manageable Risk 可管理的風險

- For the parts of cyber risk which are deemed to be insurable and manageable, overall MR exposure for the worst case loss (deemed to be a 1-in-1,000 year event loss) per scenario, is tracked against a pre-determined group-wide risk appetite

Unmanageable Risk 不可管理的風險

- Other parts of cyber risk – specifically "Infrastructure Failure" – are deemed not within appetite
- **Cyber "war",** or a massive escalation of cyber conflict between nation-states should also be excluded

IoT DDoS Botnet

Internet & telecommunications infrastructure

Source: https://www.submarinecablemap.com/

NotPetya as Wake-up Call
Notpetya 網路攻擊視為警示

Munich RE

- Russia's 2017 destructive malware attack illustrated how state-sponsored incidents can unpredictably:
  - Spill across borders, whether intentionally or unintentionally
  - Cause very large losses to individual victims
  - Cause correlated losses across sectors/countries
  - Reveal silent cyber exposure
  - Lead to wording disputes
- NotPetya created an impetus for action and reform.

A Changing Threat Environment
資安攻擊的樣態及程度不斷變動

Munich RE

- In recent years, state-sponsored cyber operations have:
  - Been carried out by a growing number of states
  - Occurred both during and outside of "war"
  - Caused increasing levels of damage to larger sets of civilian/commercial victims
- Clarifying coverage for state-sponsored incidents is more important than ever.

How Attribution Has Evolved
資安事件的歸因演變

Munich RE

- Attributing incidents to specific perpetrators and responsible states is often possible but sometimes complicated, contested, or delayed.

- Growing attribution capability among governments and private firms
- Sometimes competing voices and debates
- Confidence levels, specificity, and timelines can vary

- Insurance must anticipate how, when, and by whom attribution will occur.

Previous Wordings Challenged
先前的保單條款受到挑戰

Munich RE

- In wake of NotPetya, traditional war exclusions became subjects of litigation.

- Dearth of legal precedents
- Legal disputes still continue
- Litigation can be costly, time-consuming, and uncertain for all parties

- All parties stand to benefit from modernized cyber wordings that are clear, intentional, and relevant to today's risk environment.

Calls for New Language
新保單條款提出

Munich RE

Gallagher Re

- July 2019: "The historically well-defined line between excluded acts of war and otherwise covered perils has become blurred in the context of cyber."

THE GENEVA ASSOCIATION
IFTRIP

- July 2020: "The diversity of coverage and lack of a clear framework upon which cyber terrorism and cyber war are understood make them nebulous insurance concepts."

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

- Oct 2020: "The [traditional] war exclusion is not well-tailored to today's cyber risk landscape… New frameworks are needed."

Clarification of Cyber War 網路戰爭的新釋義
Collaboration to adapt to the new digital world 攜手走向新的數位領域

Munich RE

What are we seeking to achieve?	To clarify the scope of the war exclusion, to avoid a current or future systemic accumulation risk arising from hostile state-sponsored cyber attacks.
Why is there a need?	1. Accumulation: War or warlike events have been recognised by the insurance industry as a **significant systemic accumulation risk** across all lines of business. 2. Changing Threat: • Traditional war exclusions still used in Cyber wordings (e.g. NMA) were drafted between 1938 to late 1990s, when **no one could foresee that cyber attacks could reach the level of detrimental impact** it can have today. • State-sponsored attacks have been carried out during and outside of war. 3. Attribution Has Evolved: There is a growing attribution capability among governments and private firms.

Therefore traditional war exclusions with focus on conventional physical war are not fit for purpose to eliminate the potential of a systemic state- sponsored cyber attack.
We as an industry need to come together to form a solution to ensure that wordings are clear, intentional and relevant to today & future risk environment.

Clarification of Cyber War 網路戰爭的新釋義
How can we achieve this clarity 我們如何能達到清楚的境界

Munich RE

Initial thoughts 初步想法

A specific Cyber War exclusion must prevent **uncontrollable accumulation risk** and at the same time consider the interest of the insured being sufficiently protected against a "normal" Cyber attack(s) which is the purpose of their coverage.

Conventional War (Physical)
傳統戰爭(實體)
Including cyber attacks as a means of warfare

Attribution (歸因)
Linking cyber attacks to a sovereign state ("…by or on behalf of…")

Intolerable Detrimental Impact
無法容忍的不利影響
Severe disruption of essential services resulting in serious threats to the functioning of the public sector (e.g., administration, financial services, healthcare)

Distinction between Disruptive vs Destructive Disruptive 及 Destructive 差別
Threshold should not exclude losses from ordinary cyber espionage or singular attacks from non-state sponsored criminals.

The goal is to still provide coverage in most disruptive cases; but we need to think ahead of the technological advancements and how it can be manipulated by nation states in the course of war in the future

Thank you for your attention.

MR Greater China team/ MR Cyber tream

Munich RE