Cyber Insurance an Underwriter's Perspective

Singapore Actuarial Conference 28 August 2024

Andrew Taylor Senior Vice President,
MSIG Asia Pte Ltd
Singapore

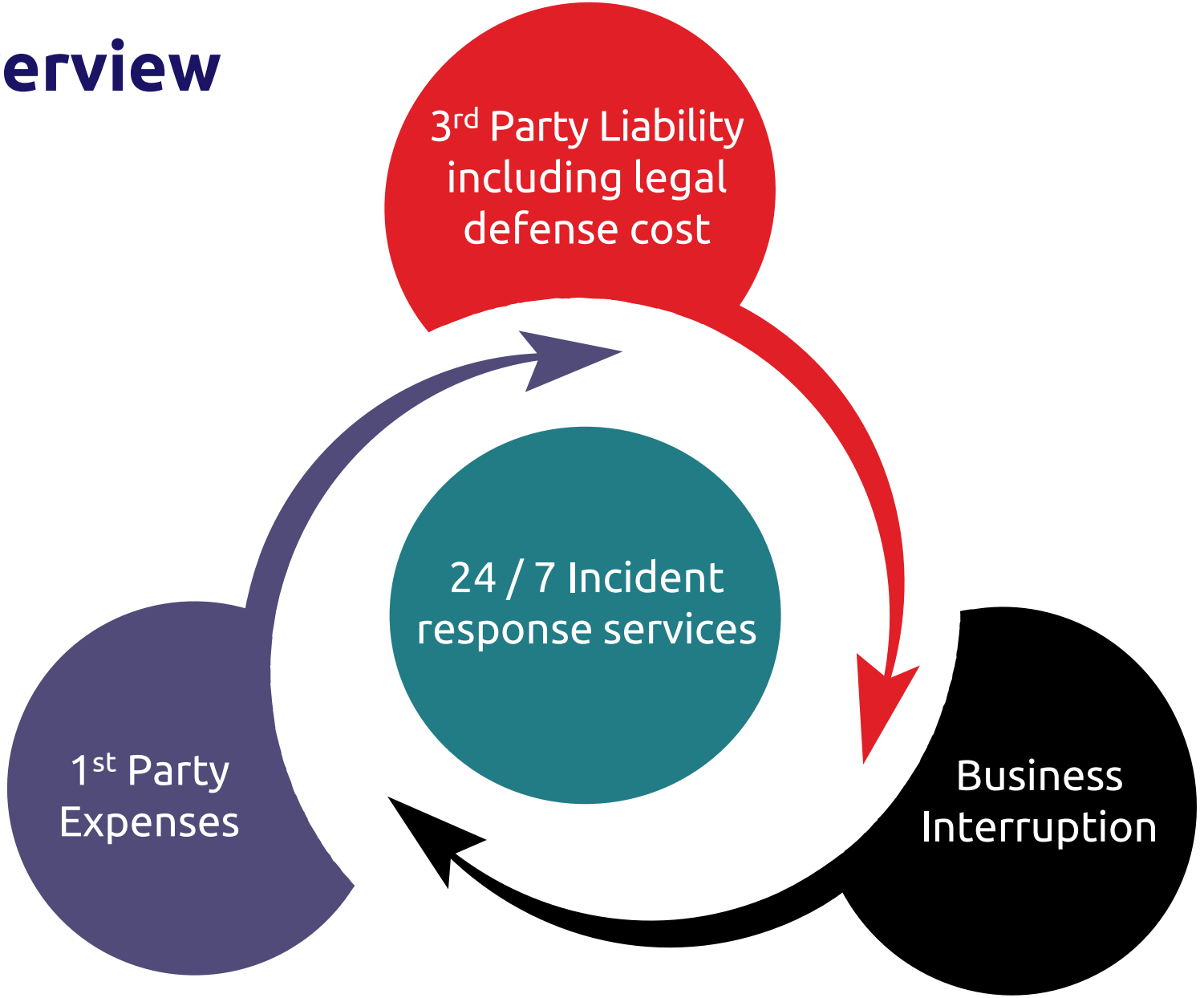
A Member of MS&AD INSURANCE GROUP

Cyber Insurance Overview

Cyber is a package insurance product

- Liability
- Business Interruption
- Expenses

Fills the gap in traditional insurance policy and meets the needs of the digital age



A MINDSET SHIFT and the insurance revolution – cyber

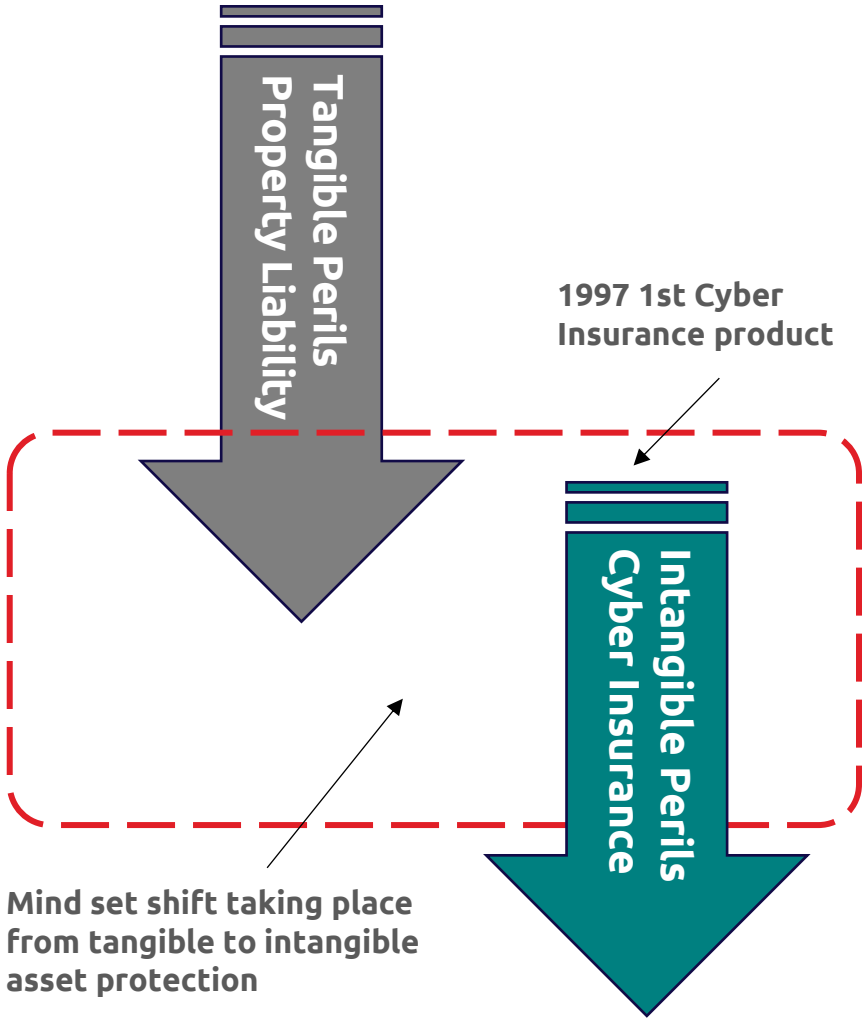
Coal 1750 – 1800
discovery of coal and its mass extraction, as well the development of the steam engine and metal forging The production line. Canal transportation

Gas 1800 – 1969
discovery of electricity, gas and oil. the combustion engine. Both steel- and chemically based products entered the market during this time. Developments telegraph and later the telephone. the plane and car.

Nuclear 1969 – 2005
Nuclear energy and electronics enter the landscape.
The internet and age of personal PC's a shift from paper to server to cloud.

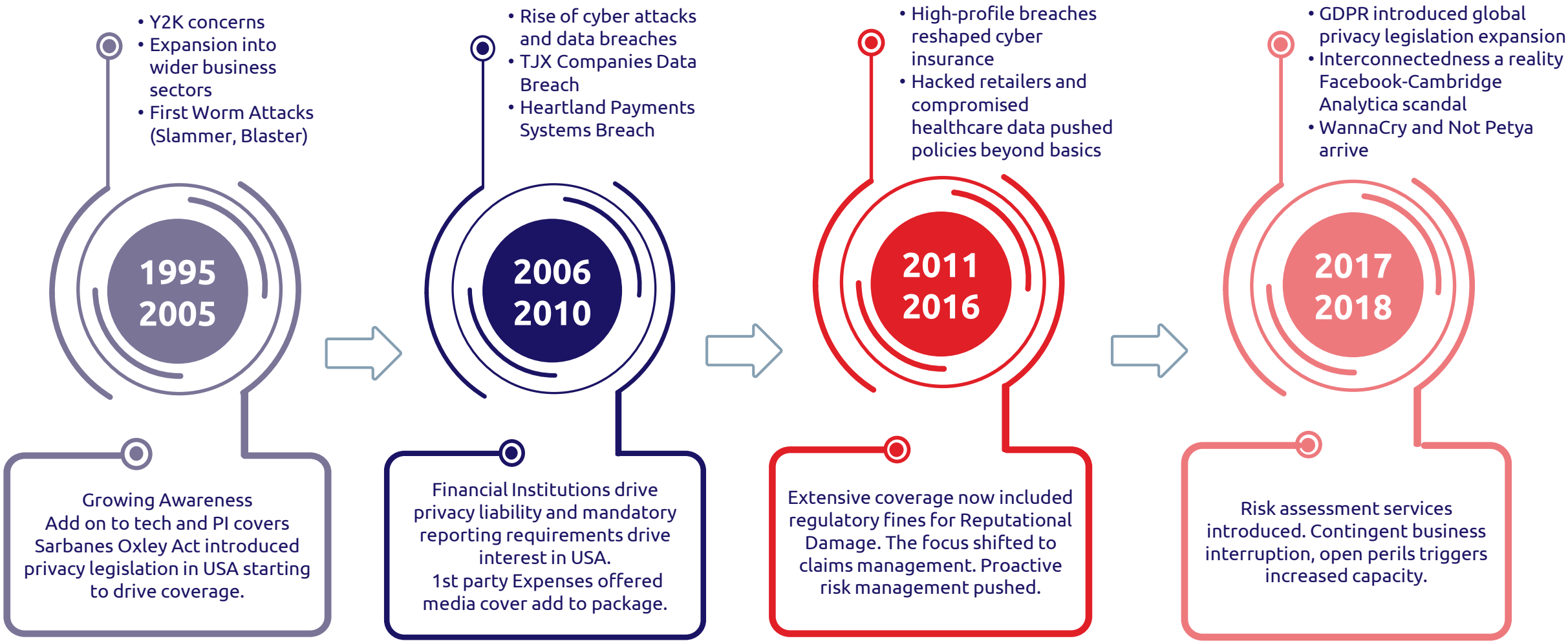
IoT 2005 -
Faster computers and telecommunications real-time connection within more and more components of production line, both inside and outside facility walls. Industrial Internet of Things, cloud technology and artificial intelligence continue. A virtual world will merge with the physical world.

https://www.upkeep.com/learning/four-industrial-revolutions



Cyber insurance history

Cyber insurance evolution



Major cyber attacks and data breaches / malware strains 2000's

ILOVEYOU Worm (2000):

Impacted 45 millions computers worldwide, estimated damage $10 billion.

SQL Slammer Worm (2003):

Affected over 75,000 victims within 10 minutes.

Mydoom Worm (2004):

25% of global emails infected.

Zeus Trojan (2007):

Targeted thousands of businesses, stealing banking information.

Data Breaches

Heartland Payment Systems (2008):

Exposed data of over 100 million credit card transactions.

Aurora Attack (2009):

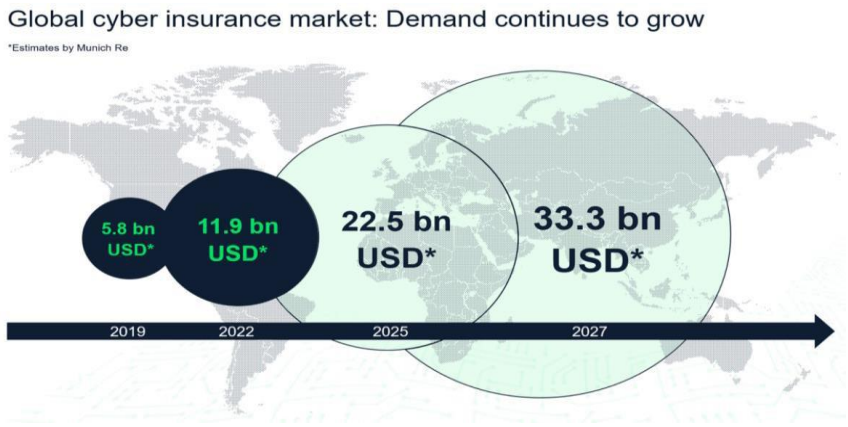
Targeted major companies like Google and Adobe

Cyber Insurance Market

Size and Trend

	GLOBAL	APAC
GWP	2023: 12 Billion 2032: USD 117 Billion[1]	2023: USD1.1Billion 2032: USD 8.2 Billion[2]

Market Insights



"**APAC** is expected to witness **significant growth** during the forecast period owing to **increasing ransom attacks and risks** in the region."

- Fortune Business Insights

"**APAC** is projected to be the **fastest-growing region** for the **cyber insurance** market during the forecast period."

- Allied Market Research

"**Fastest growth** area of insurance by some distance."

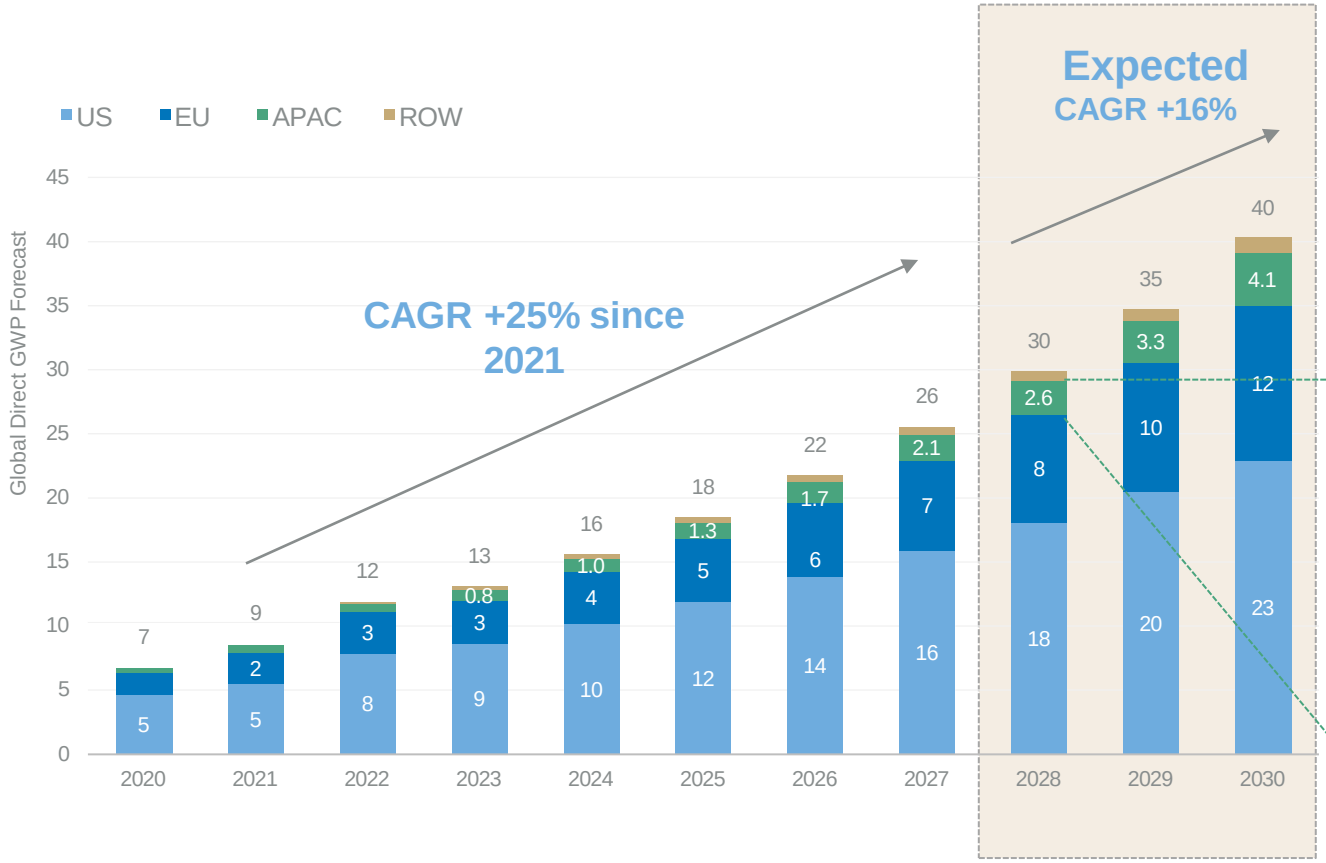
- Howdens

CAGR (Over 10 years)	25 – 30%[3]	51%[3]

1. Allied Market Research
2. Gallagher Re internal research = A Taylor extrapolation
3. S&P Report Global Cyber Insurance : Reinsurance Remains Key to Growth 29 Aug 2023

Cyber Market Growth - Corporate

Market Size Estimate



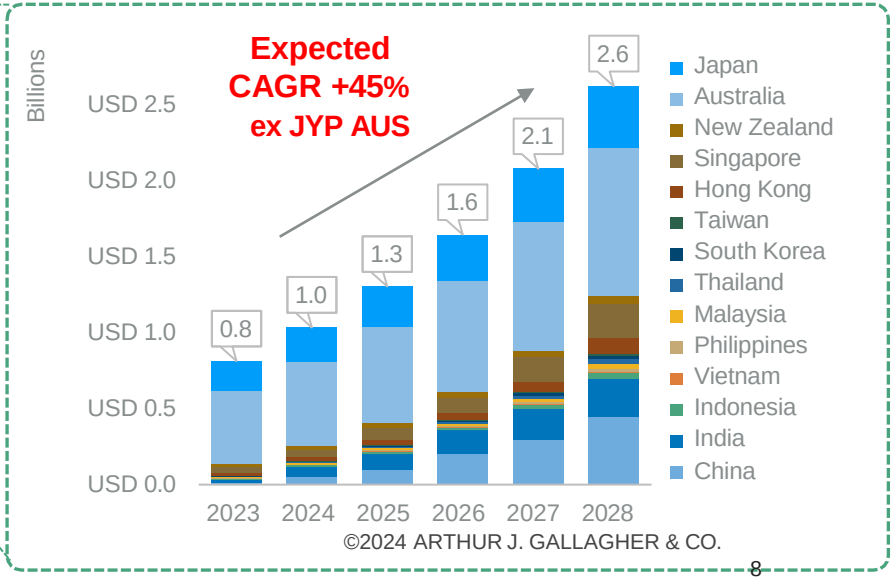
Source: Gallagher Re estimates.

Swiss Re says cyber to be 'as big as property' by 2040

Factors driving growth

- Better understanding of the exposures
- Increased frequency and sophistication of cyber-attacks
- Growing regulatory requirements
- Higher awareness and adoption among businesses
- Greater digital use and need

APAC Focus:



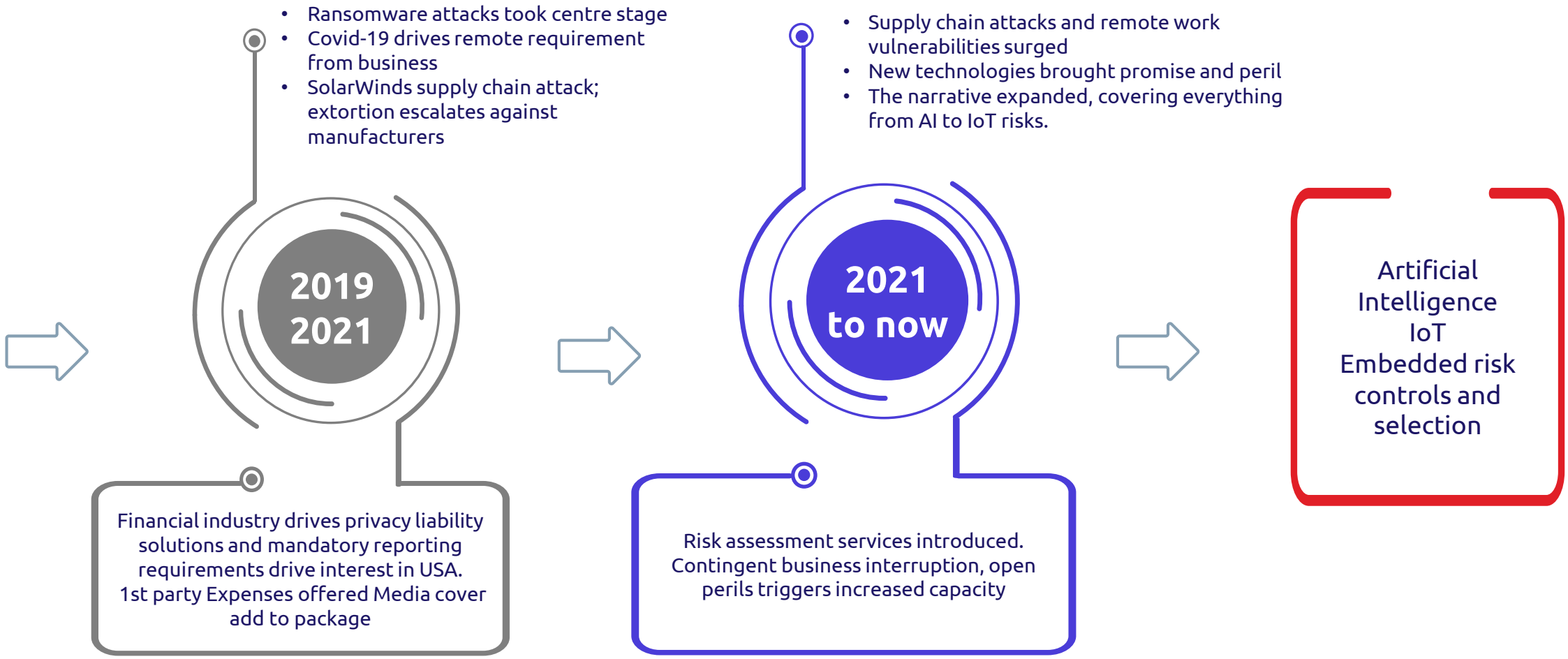
Major cyber attacks and data breaches / malware trains 2010's

- **Stuxnet (2010):** Targeted Iran's nuclear facilities, impacting SCADA systems.
- **WannaCry Ransomware (2017):** Affected over 200,000 computers across 150 countries.
- **NotPetya Ransomware (2017):** Caused billions in damages globally.

Data Breaches

- Sony Pictures Hack (2014)
- Anthem Inc. Data Breach (2015): 78.8 million people.
- Equifax Data Breach (2017): 147 million people.
- Marriott Data Breach (2018): 500 million guests.
- SingHealth (2018): 1.5 million patients.
- Capital One Data Breach (2019): 100 million customers.
- Cathay Pacific (2018): 9.4 million passengers.

Cyber insurance evolution



Major cyber attacks and data breaches / malware trains from 2020's

- **SolarWinds Attack** (2020): Compromised numerous U.S. government agencies and businesses[3].
- **Colonial Pipeline** Ransomware (2021): Disrupted fuel supply across the U.S. East Coast.
- **Kaseya VSA** Ransomware (2021): Impacted up to 1,500 businesses.
- **Log4Shell** Vulnerability (2021): Affected millions of devices globally.
- **Microsoft Exchange Server Hack** (2021): Compromised over 30,000 organizations in the U.S. alone

Data Breaches

- **Facebook** Data Breach (2021): 530 million users
- **T-Mobile** Data Breach (2021): 40 million customers.
- **Accellion** Data Breach (2021): Impacted multiple organizations, exposing sensitive data.
- **JBS Ransomware** Attack (2021): Disrupted operations of the world's largest meat processing company.
- **Tokopedia** (2020): 91 million users.
- **Singtel Optus** (2022): 9.8 million customers.

Cumulative computer vulnerabilities

Share of attacks by industry 2019–2023

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and insurance	18.2%	18.9	22.4	23	17
Professional, business and consumer services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and telecommunications	1.2%	0.5	2.5	5.7	10

Ransomware Accounted for 17% of incidents .

Manufacturing region saw the most incidents in

- ***Asia Pacific*** (54%).
- Europe at (26%),
- North America (12%) and Latin American (5%).

Finance & Insurance

- Europe 37%
- Latin America 17%
- America Asia

Energy

- 43% of incidents involved malware. Data Theft 33% Ransomware 22%

Global event considerations

A wake UP Call

- 27 June 2017 **NotPetya** cyber attack
- allegedly **Russian** threat actors
- The malware **wiperware** (not ransomware)
- cost **around $3 billion across** various insurance policies, including both affirmative cyber insurance and **silent** non-affirmative policies.
- **Systemic Risk** can into greater focus.
- the event emphasised the need for clearer and more comprehensive cyber insurance policies that explicitly address the evolving landscape of cyber risks.

THE MARKET AND INDUSTRY RESPONSE

London Market Association (LMA)

November 2021, 2022 and 2023 ……

Cyber War and Cyber Operation Exclusion Clauses

LMA5564A - War, Cyber War and Cyber Operation Exclusion No. 1
LMA5565A - War, Cyber War and Limited Cyber Operation Exclusion No. 2
LMA5566A - War, Cyber War and Limited Cyber Operations Exclusion No. 3
LMA5567A - War, Cyber War and Limited Cyber Operation Exclusion No. 4

The MARKET AND INDUSTRY RESPONSE

- **Mondelez International**

- **Merck & Co.**

The court held that “no court has applied a war (or hostile acts) exclusion to anything remotely close to the facts herein” and while ….. **Cyber attacks of various forms**, sometimes from private sources and **sometimes from nation-states** have become more common Merck had every right to anticipate that the **exclusion applied only to traditional forms of warfare”.**

A Traditional War exclusion

Directly or indirectly occasioned by, happening through or in **consequence of war**, invasion, **acts of foreign enemies**, **hostilities** (whether war be declared…..) of any government or public or local authority, except that this exclusion **shall not apply to cyber terrorism**" or not), civil war, rebellion, revolution, insurrection, military or usurped power or confiscation or nationalisation or requisition or destruction of or damage to property by or under the order

Challenges

Kinetic debate

Attribution debate

Declared

Cyber Terrorism

LMA 5567A extract

War exclusion

…….

1. that part of any loss, damage, liability, cost, or expense, of any kind:

    1. directly or indirectly arising from a **war**, and/or
    2. arising from a **cyber operation** that is carried out as part of a **war**, or the immediate preparation for a **war**, and/or
    3. arising from a **cyber operation** that causes a **state** to become an **impacted state**.

    *Paragraph 1.3 shall not apply to the direct or indirect effect of a **cyber operation** on a **computer system** used by the **Insured Organisation** or its third party service providers that is not physically located in an **impacted state** but is affected by a **cyber operation**.*

    …….

Challenges

Impacted State

Major detrimental impact

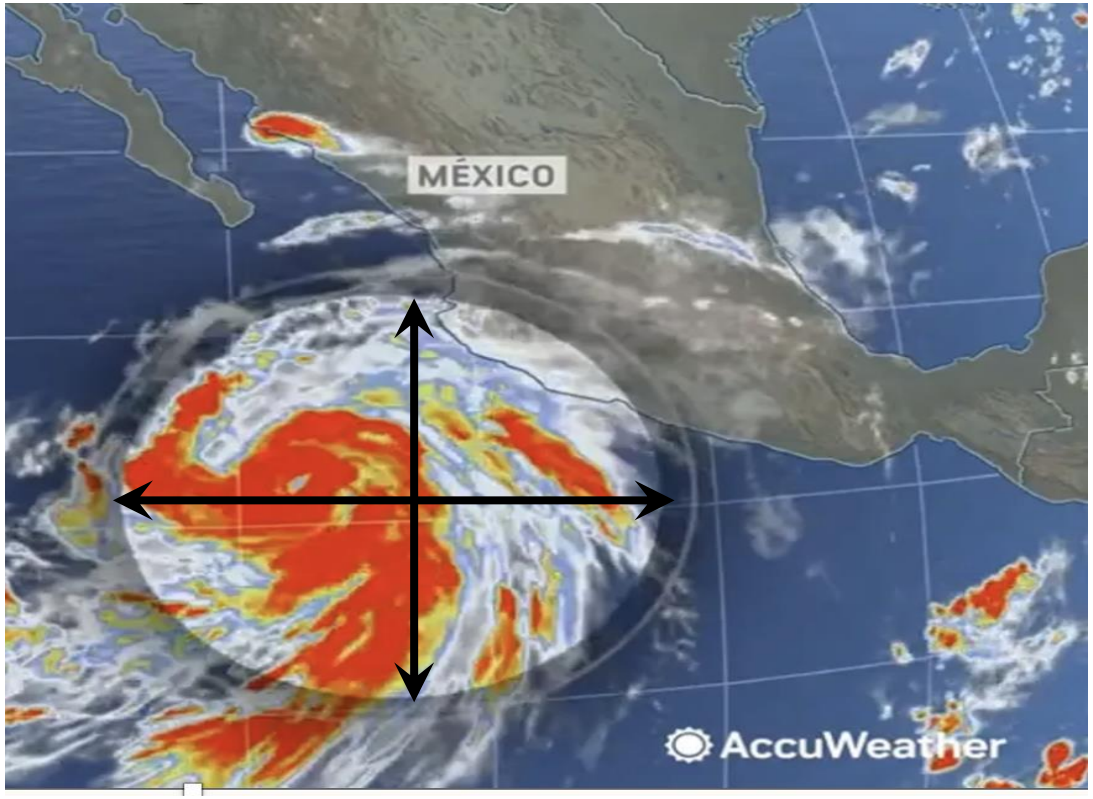
Attribution

Timing of payments

Cyber Terrorism

Cyber Operation

What's Next



- Sustainability or the market is at risk
- Continued refinement and debate
- We must educate our clients of the issues

Underwriting cyber insurance

Underwriting Cyber Risks

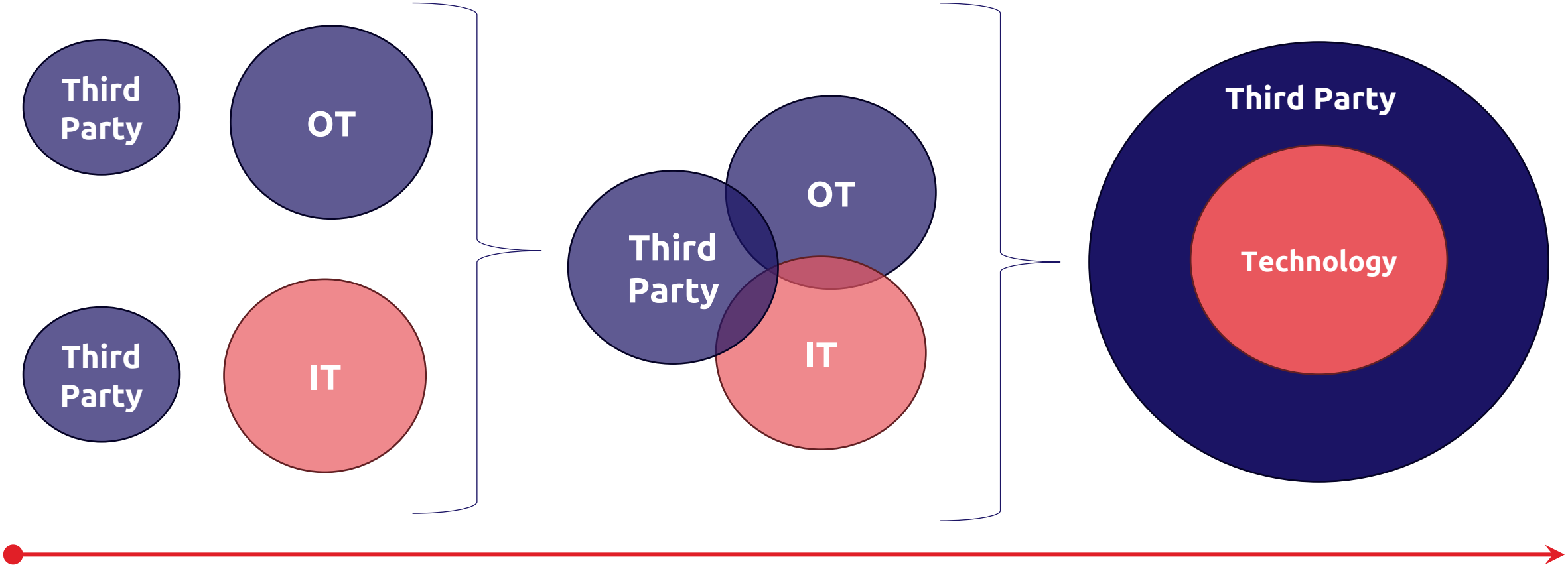
Basics	• Revenue • Number and type of records • Industry
Culture	• Senior executive dedicated to data management • Board approved data management policy
Records Management	• Detect – Type and amount of information • Protect – How is the data protected? • Plan – Board approved information security program
Network Operations	• Patch management, BCP, IDS, back up and testing • Review of network and security assessments • Volume and activity
Regulatory Compliance	• Number and type of regulations • How long compliance has been achieved
Vendor Management	• Due diligence if vendors and service providers • Contract management
Loss Experience	

Information Technology vs Operational Technology

-

Business Priorities	
1. Confidentiality	1. Availability
2. Integrity of Data	2. Integrity of Data Configuration
3. Availability	3. Confidentiality

A maturity model to manage Risk Convergence



Closing thoughts

Current State of the Cyber Insurance Market

- The cyber insurance is still experiencing growing pains, such as capacity fluctuations and debates over policy wording
- The demand for cyber insurance continues to grow and there remains high with uninsured risks still the major opportunity.
- There will continue to be a focus on sustainable insurability and market functionality to meet this increasing demand.

Current Market Concerns

- Ransomware: Ransomware attacks remain a significant concern, with attackers becoming more sophisticated and demanding higher ransoms.
- Regulatory Changes: Evolving regulations around data protection and privacy are impacting the cyber insurance market.

Potential New Exposures

- IoT and Smart Devices: The proliferation of Internet of Things (IoT) devices introduces new vulnerabilities for insurers understand.
- Artificial Intelligence (AI): While AI can enhance cybersecurity, it also introduces new potential threats.

Overall, the cyber insurance market is navigating a complex landscape of evolving threats and regulatory changes. Insurers must continue to adapt their strategies to manage these risks effectively and provide comprehensive coverage to their clients.