



The webinar will begin soon.

While you wait, explore IRMI's extensive collection of resources focused on the complexity and nuances of cyber insurance....



### ***The Betterley Report***

A series of highly acclaimed market survey reports on six specialty insurance products, including cyber, technology, errors and omissions (E&O), private company management, and employment practices liability (EPL) insurance.



### ***Specialty Lines Compass***

Each month, you will receive summaries on the latest developments affecting directors and officers (D&O) liability insurance with insightful tips for arranging broad coverage.



**Management Liability Insurance Specialist (MLIS®)**  
Understand the ins and outs of management liability insurance with courses covering cyber and privacy liability exposures, EPL, fiduciary liability, and D&O liability and exposures.

**Learn More at [IRMI.com/SpecialtyLines](https://IRMI.com/SpecialtyLines)**

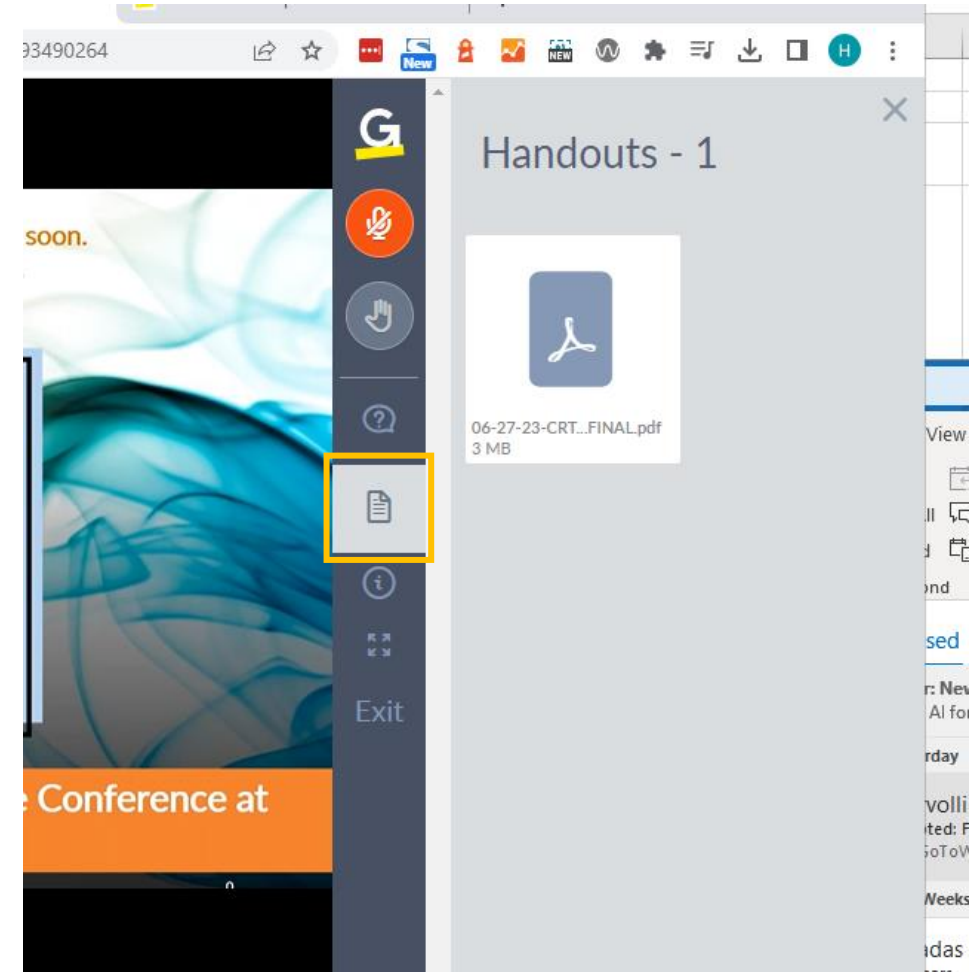
# Get the PowerPoint Handouts

## Handouts

---

You can access the webinar slides in PDF format from the Handouts pane or icon.

- Navigate to the Handouts pane or icon.
- Click the handout you want to access.
- The file will automatically start downloading from your default Web browser.
- Click the downloaded file to open or save it.

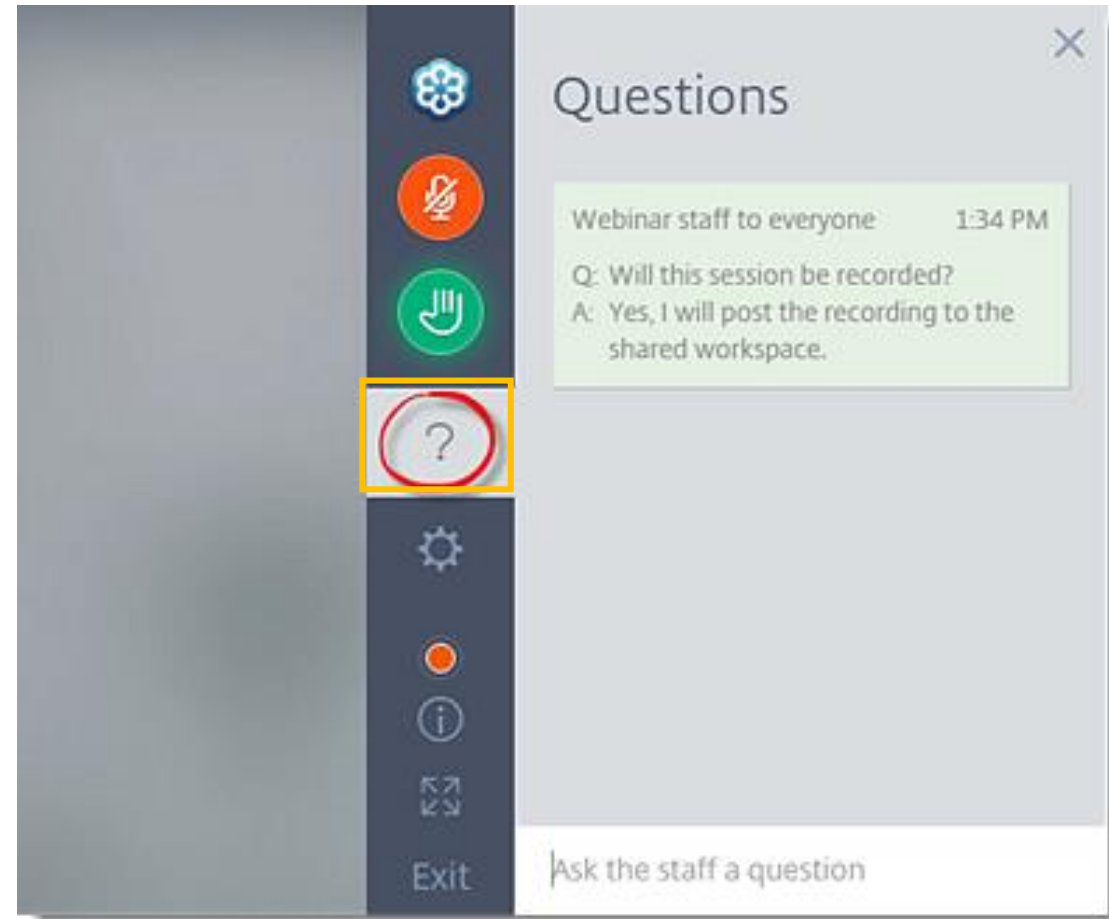


# GoTo Webinar Attendee Participation

## Questions

Type a question or comment into the Questions box and click Send.

Mobile: you may need to tap on the screen to see options.



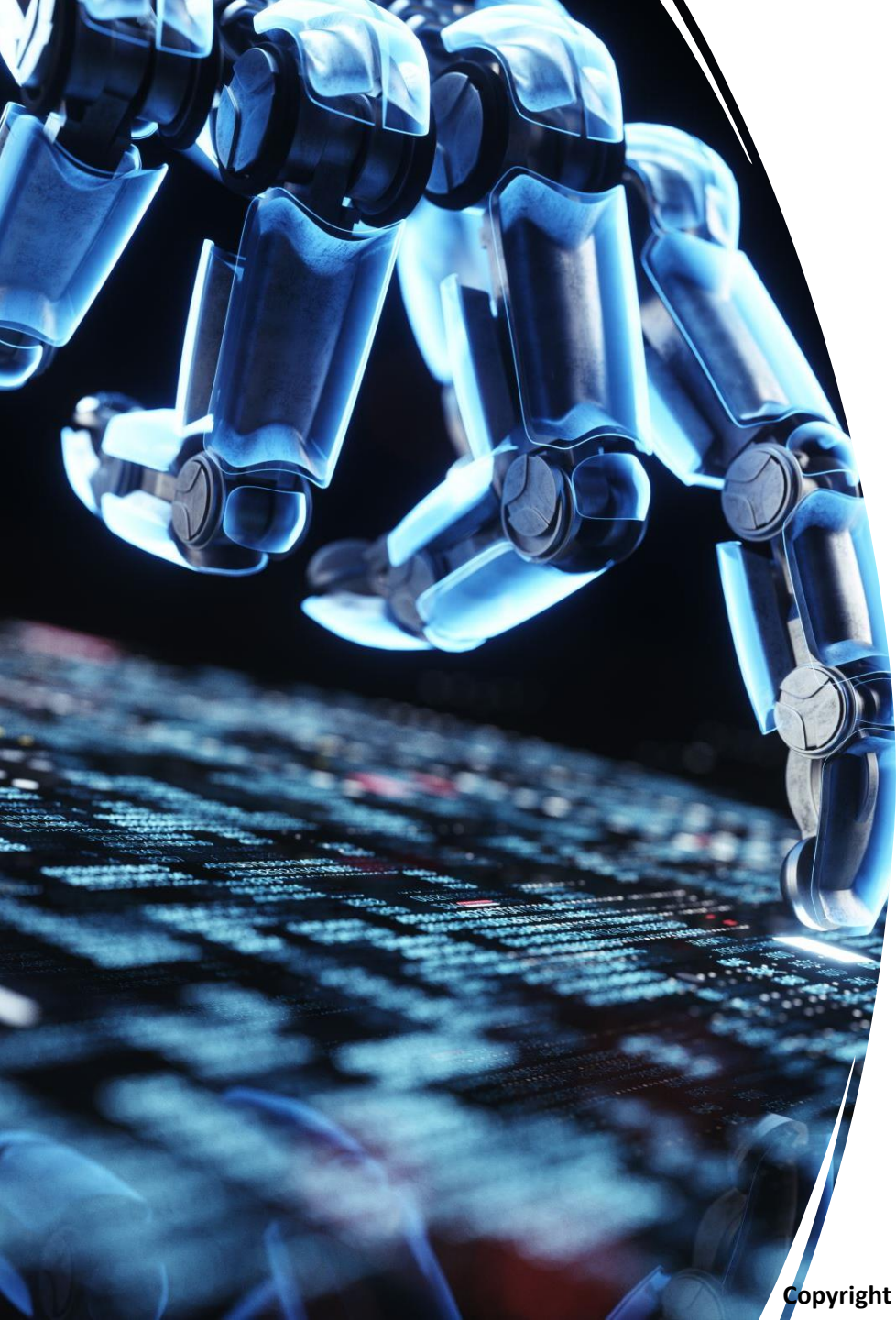
# Your Webinar Presenters



**Richard Betterley**  
Betterley Risk Consultants  
Email: [rbetterley@betterley.com](mailto:rbetterley@betterley.com)



**Jes Alexander**  
IRMI  
Email: [Jes.A@IRMI.com](mailto:Jes.A@IRMI.com)



# The Latest Impactful Trends in Cyber Insurance

---



# What Is *The Betterley Report*?



- Survey of six specialty insurance markets and the leading insurer's products in each market
  - **Cyber insurance**
  - Employment practices liability insurance
  - Cyber insurance for healthcare
  - Private company management liability insurance
  - Intellectual property and media liability insurance
  - Technology errors and omissions insurance
- Reviews the state of the market, including pricing trends
- Detailed policy comparison charts citing the key differences among insurers, such as market focus, capacity, coverage wordings, and value-added services



# The State of the Cyber Market: the Insurers in Our Survey

---

- Almost all participants plan some rate decrease—from a low end of flat to down 10 percent.
- Only one was planning flat and none an increase.
- Deductibles are expected to remain flat.
- Growth rates were negative for most.
- Finally, reinsurance availability seems stable.

# The State of the Cyber Market



- In the US market generally, 2023 direct written premiums were between \$10.4 billion–\$11.5 billion, compared to \$10.0 billion in 2022.
- ↑ Stand-alone cyber policies in force grew by 18 percent.
- ↓ Greater than a 3 percent drop in direct written premiums.
- Stand-alone cyber policies in force would reach a milestone 500,000 mark in late 2024 or early 2025.

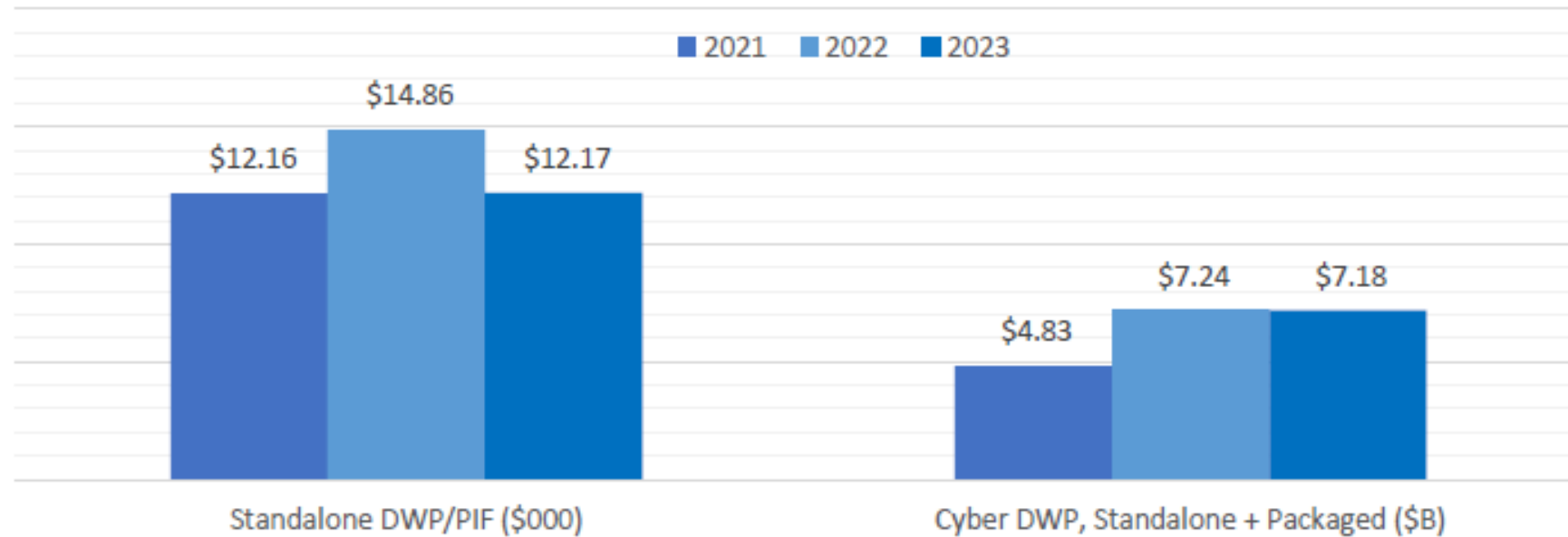
*Source:* Verisk Underwriting Solutions/MarketStance analysis of NAIC Cybersecurity and Identity Theft Insurance Supplement Data



# The State of the Cyber Market



## More Small Commercial Insureds and Rate Moderation



Source: Verisk Underwriting Solutions/MarketStance analysis of NAIC Cybersecurity and Identity Theft Insurance Supplement Data

# The Broadening of the Cyber Market



- Contracts require small and midsize businesses to maintain cyber insurance as a condition of doing business.
  - Examples: vendors, lenders, and clients
- Coverage requirements are becoming an issue.
  - Some business agreements are punitive to small and midsize insureds, as they require unreasonable limits or seek to hold the companies responsible for *unlimited* losses.
- Will commercially reasonable requirements for cyber insurance develop over time?

# Cyber-Market Concerns



- Ransomware
- Deceptive funds transfer
- Extortion events
- \*Governmental regulations restricting ransom payments

# Market Concerns: Continued Increase in Ransomware



- What are the three main drivers of the increased frequency of ransomware attacks?
  - Work-from-home policies make cyber security more difficult for companies.
  - Inflation and insufficient staffing are impacting cyber security.
  - Increased focus on delivering goods and services online.



# The Tech-Forward Approach



- How important is a “tech-forward” approach to cyber?
  - Data and risk control services provided to insureds to mitigate potential claims
- The acquisition of Corvus by Travelers

# Tables in *The Betterley Report*



- Contact and Product Information
- Product Description
- Market Information
- Capacity, Deductibles, Coinsurance, and Agent Access
- Data Privacy: Types of Coverage and Limits Available
- Data Privacy: Regulatory and Statutory Coverage Provided
- Data Privacy: Payment Card Industry Coverage Provided
- Data Privacy: Coverage Triggers
- Data Privacy: Types of Data Covered
- Data Privacy: Remediation Costs Covered
- Data Privacy: Remediation Coverage Services
- Coverage Extensions and (Sub)Limits Available for Cyber Insureds—Media Liability
- Product Features Related to AI Exposures

# Tables in *The Betterley Report*



- Security Assessment by Third-Party Requirements
- First-Party Coverage: Direct Damage and Business Interruption
- Coverage for Loss Resulting from a State-Sponsored Act
- Coverage for Loss Resulting from a Non-State-Sponsored Terrorist Act
- Theft (First-Party) Coverage
- Theft (First-Party) Coverage—Deceptive Funds Transfer or Social Engineering
- Third-Party Coverage: Bodily Injury and Property Damage
- Third-Party Coverage
- Claims Reporting, Extended Reporting Period, Selection of Counsel, Consent To Settle
- Prior Acts
- Coverage Territory
- Exclusions
- Risk Management Services

# First-Party Cyber Coverages

---





# Deceptive Funds Transfer Coverage

---

- The deceptive fund transfer table includes the following information for each insurer.
  - The maximum limit available
  - The nature of the electronic missive covered (e.g., email, text, instant message, phone)
  - Whether electronic funds transfer fraud of the insured's funds is covered
  - Whether coverage is offered for a customer's loss of funds if they were deceived via a fraudulent communication purporting to be from the insured
  - Whether coverage is offered for a customer's loss of funds having bought from a website purporting to be yours

# Deceptive Funds Transfer Coverage



## Theft (First-Party) Coverage—Deceptive Funds Transfer or Social Engineering

Insurer	Maximum Limit	Sublimit, If Any?	Nature of Electronic Missive Covered (i.e., Email, Text, Instant Messaging, Phone, etc.)?	Electronic Funds Transfer Fraud of the Insured's Funds Covered?	Cost To Reimburse Customer's Funds for Their Loss Arising Out of Fraudulent Communication Purporting To Be from You	Cost To Reimburse Customer's Funds for Their Loss Arising Out of Fraudulent Websites Purporting To Be Yours
<b>AIG</b>	Varies by risk and segment	Varies by risk and segment	Coverage available for multiple modes of communication via Impersonation Fraud Coverage Endorsement, Crime or Fidelity Policy	Available via Cyber Crime Endorsement	Available via Cyber Crime Endorsement	No
<b>Allied World</b>	\$1 million	Typically \$100,000	No restrictions	Yes	No	No
<b>At-Bay</b>	Varies by risk	Typically sublimited	Any electronic communication	Yes	Yes	No
<b>Beazley</b>	Varies by risk	Varies by risk	All forms including written, electronic (including email or web-based), or telephone	Yes	No	No

# Cyber Coverages: Theft of Intellectual Property



- Theft of the economic value of intellectual property (IP) is a major exposure from data breaches.
- Thefts can include trade secrets, source code, customer lists, etc.
- Rise in employee IP theft.
- Coverages not well developed.

# Cyber Coverages— Theft of Intellectual Property

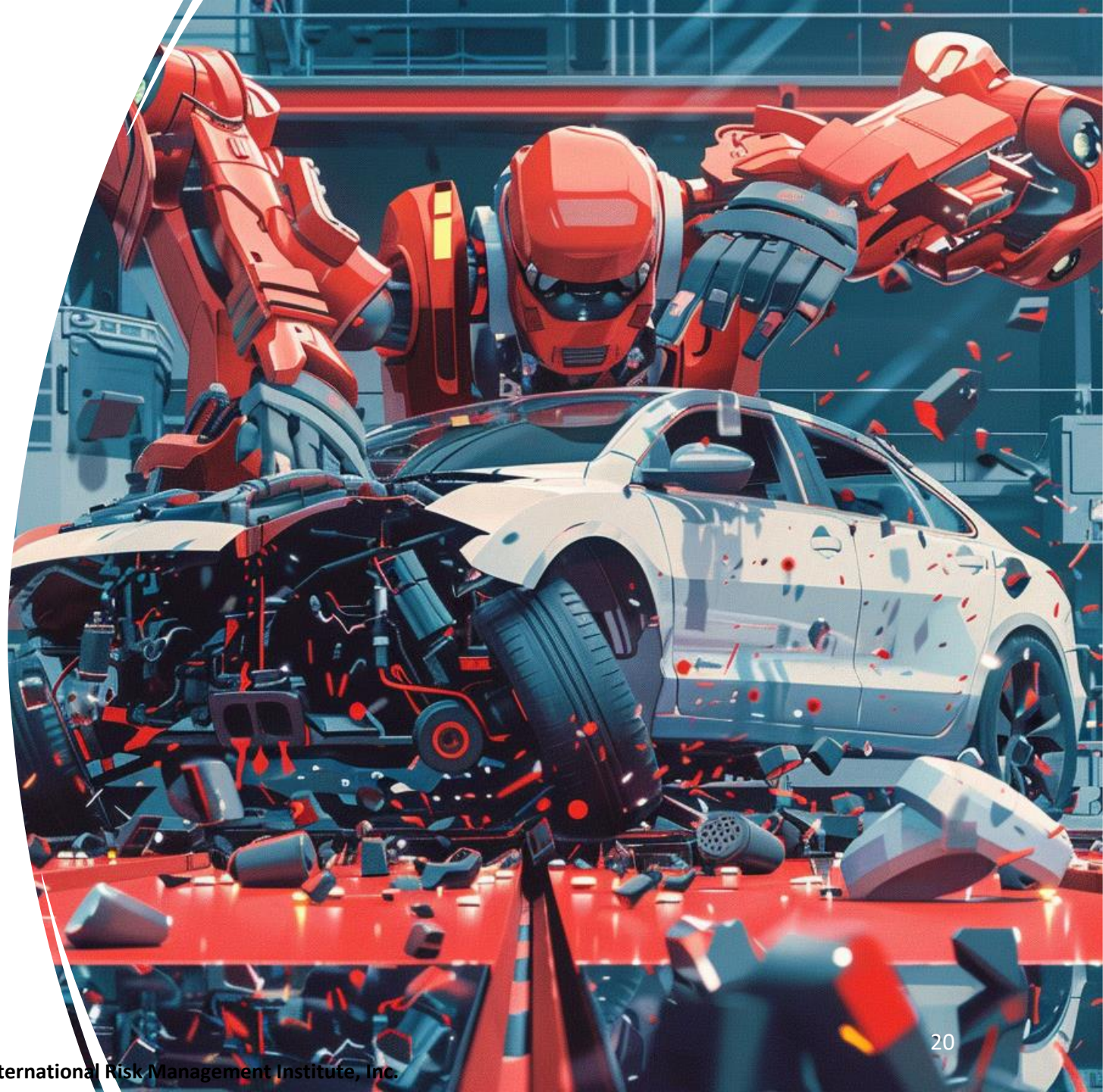


Theft (First-Party) Coverage						
Insurer	Theft of Data	Theft of the Economic Value of Intellectual Property	Theft of Money or Securities	Theft of Finished Goods or Work in Process	Extortion	Theft of Computing Resources
<b>AIG</b>	Yes	No	No	No	Yes	Potentially network interruption or event response, if a Security Failure. Computer Fraud, Telephone Fraud, and Cryptojacking available by endorsement
<b>Allied World</b>	Yes	No	Yes, via Cyber Crime	No	Yes	Yes, via Network Interruption coverage
<b>Berkshire Hathaway Specialty</b>	Yes	No	No	No	Yes	No
<b>Celerity Pro</b>	Yes	No	Yes, as it relates to Social Engineering and Funds Transfer Fraud.	No	Yes	No, unless resource is a data asset. Telecom Fraud coverage available via endorsement.



# Third-Party Cyber Coverages

---



# Cyber Liability for Bodily Injury and Property Damage



- Traditionally, direct bodily injury and property damage losses were not covered by cyber policies.
- Why is coverage for bodily injuries and property damages important under a cyber policy?
- Some cyber insurers have added coverage for bodily injury and property damage.

# Cyber Liability for Bodily Injury and Property Damage



## Third-Party Coverage: Bodily Injury and Property Damage

Insurer	Bodily Injury		Property Damage	
	Direct	Contingent	Direct	Contingent
<b>AIG</b>	Yes, available through CyberEdge PC or CyberEdge Plus	Yes, available through CyberEdge PC or CyberEdge Plus	Yes, available through CyberEdge PC or CyberEdge Plus	Yes, available through CyberEdge PC or CyberEdge Plus Casualty
<b>Allied World</b>	Mental Anguish Emotional Distress Carveback	No	No	No
<b>At-Bay</b>	No	Yes, available via endorsement	Yes, available via Bricking Endorsement	No
<b>Beazley</b>	No	Contingent bodily injury is available to select insureds via endorsement subject to underwriting	No	Contingent property damage is available to select insureds via endorsement subject to underwriting





# AI's Impact on Cyber Insurance



# AI May Increase Cyber Attacks



The rise of generative artificial intelligence (AI) will likely increase the frequency of cyber attacks, especially social engineering.

- **Phishing attacks.** Generative AI can craft cunning messages without the grammatical flaws that characterize many current phishing attempts. Language barriers will be removed, and hackers can create bots that respond in real time.
- **Deepfakes.** Generative AI has the ability to clone voices and create realistic videos, which can be utilized by attacks to deceive employees into initiating fraudulent wire transfers.
- **Data mining.** AI's ability to improve and automate data mining will amplify cyber attacks, as the gathering of company-related information will become even easier.



# Enter the Malicious GPTs

A hacker version of ChatGPT already exists. WormGPT!

# Responses from Insurers on AI



- What are cyber insurers doing in response to AI?
  - Most insurers report that they are watching and evaluating the AI exposure, but ...
    - Currently, few insurers are applying policy language addressing AI.
    - No indication of exclusions or limitations.
  - A new trend? AI affirmative coverage. But is specific wording needed?
    - Coalition added an AI security event to its definition of security failure, and it added fraudulent instructions using deepfakes to its definition of funds transfer fraud.
- What risk management services are insurers offering relating to AI?
  - Vague or no responses, but that will change.

# AI and the Future of Cyber



- Will cyber insurers create AI-specific coverage limitations or exclusions?
  - Approach is problematic. How would an insurer determine an AI was involved?
  - Brokers may not recommend policies that attempt to exclude AI-caused losses, as it has the potential to exclude a wide swath of claims.
- It may just be an underwriting question: Is the applicant more at risk of a costly AI-enhanced attack?
- Potential new subrogation target for cyber insurers—the developers of AI models (e.g., OpenAI, Google, Microsoft)



# Questions?



Thank you for attending the webinar.  
Subscribe to *The Betterley Report* now!

Make smarter decisions  
with detailed  
evaluations of specialty  
insurance products.

IRMI features six  
individual *Betterley  
Reports*.

Reports can be  
purchased individually  
or bundled together at  
a discounted rate.

Learn More at [IRMI.com/SpecialtyLines](https://IRMI.com/SpecialtyLines)





Thank you for attending the webinar.  
Explore IRMI's extensive collection of resources focused on the complexity and nuances of cyber insurance....



**Management Liability Insurance Specialist (MLIS®)**  
Understand the ins and outs of management liability insurance with courses covering cyber and privacy liability exposures, employment practices liability (EPL), fiduciary liability, and directors and officers (D&O) liability and exposures.



***Specialty Lines Compass***  
Each month, you will receive summaries on the latest developments affecting D&O liability insurance with insightful tips for arranging broad coverage.



***Professional Liability Insurance***  
This reference provides actionable recommendations and useful insight into errors and omissions (E&O), medical and nonmedical professional, and management liability exposures insurance.

**Learn More at [IRMI.com/SpecialtyLines](https://IRMI.com/SpecialtyLines)**