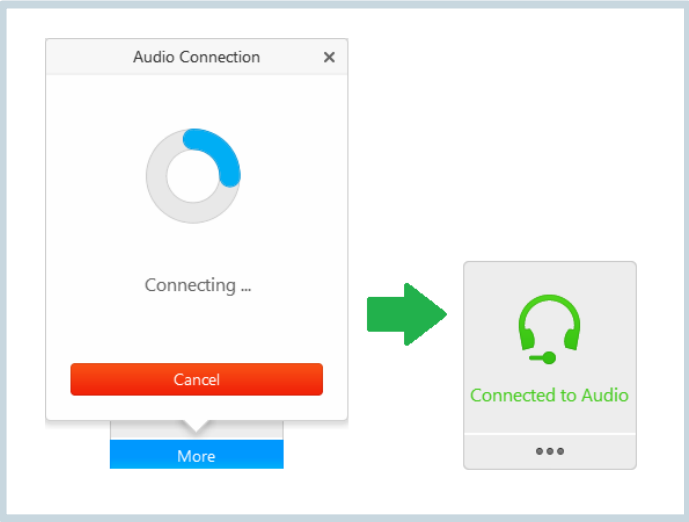
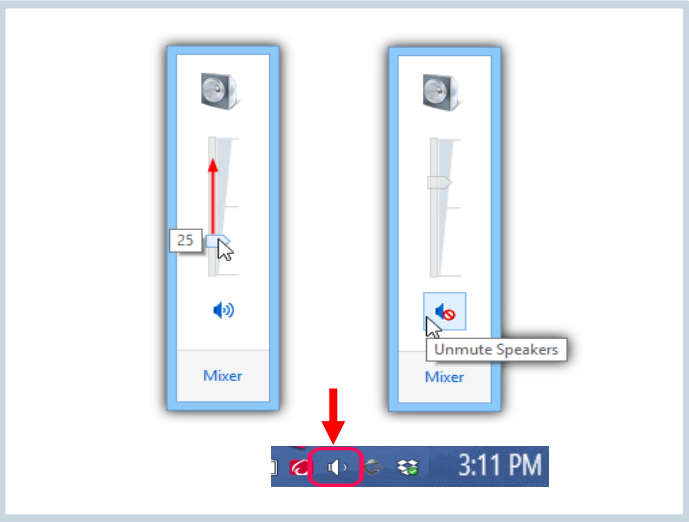
Participant information

- Telephone audio will stream through your computer speakers.
  Please make sure your computer speakers are **on** and your console is **unmuted.**



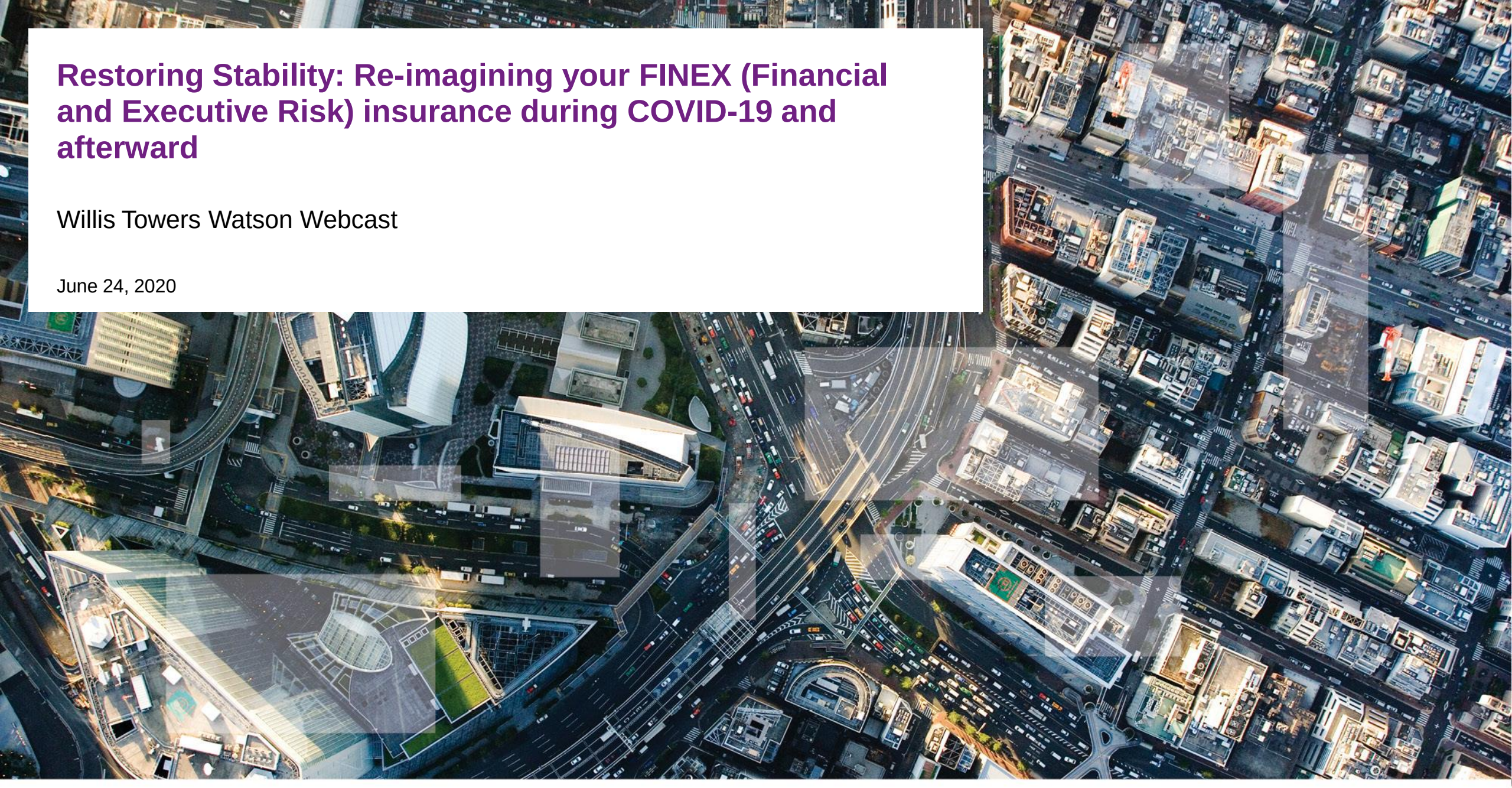


- If you are having technical difficulty hearing through your computer speakers, please use the chat to troubleshoot with the event specialist.
- To submit a question, select the Q&A panel on the left side of your screen. We will leave time at the end of the presentation for questions.
- All registrants will receive a copy of today's presentation and a link to a replay of the discussion via email.

Restoring Stability: Re-imagining your FINEX (Financial and Executive Risk) insurance during COVID-19 and afterward

Willis Towers Watson Webcast

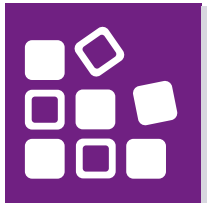
June 24, 2020



Willis Towers Watson

Today's agenda

Is your D&O coverage ready to protect your directors and officers as they lead through the crisis?



Workforce insurance, perils and trends: Employment Practices and Wage and Hour Liability

Today's coverage for tomorrow's cyber and privacy exposures

Solving claims issues in a time of crisis and hardening market

Questions and answers

Today's speakers

Chuck Shay

Midwest/West Region Leader, FINEX North America

Rob Yellen

D&O and Fiduciary Liability Product Leader, FINEX North America

Talene Carter

EPL Thought & Product Leader, FINEX North America

Joe DePaul

Head of Cyber/E&O, FINEX North America

Brian Weiss

Head of the Claims & Legal Group, FINEX North America

Directors and Officers market before COVID-19

Underlying causes of an already hardening-market

Claims

- 400+/YR SCAs
- Mega-Derivatives
- Bankruptcy
- Event Driven
- M&A-82% to 90%

Social Inflation

- Social media has an impact
- Viral campaigns with immediate impact
- Expansive corporate purpose
- Litigation funding growing

Rate trends

- 10 years or more—declining rate
- Excess markets recalibrating
- Side-A hits floors, then falls through

No more cash flow underwriting

- Historically-low interest rates
- Underwriting has to be to a profit
- 50% less public companies today than in 1998

… and then COVID-19 strikes …

Directors and Officers Liability – Exposures impacted by COVID-19

Disclosures (Public companies)

- Offerings-Strict Liability (Securities Act of 1933)
- Public Companies
  - COVID-19 Risk
  - COVID-19 Opportunity
  - Pre-COVID-19 statements, big drop, then blame anything other than COVID-19

Transactions and Transitions

- Deal failure litigation
- Restructuring
  - In court (bankruptcy)
  - Out of court
- SPAC's are back!
- Re-engineered workforce

Liquidity/Bankruptcy

- Uncertainty over the length of our COVID-19 challenges, potential new waves, exacerbate short term liquidity challenges.
- Trustee, Creditors' claims
- Carriers are concerned. Big wave(s)? Maybe a *tsunami*!

Event-Based Claims

- Cyber
- Privacy
- Social justice/Social amplification (like, #MeToo)
- Government investigations
- Consumer protection

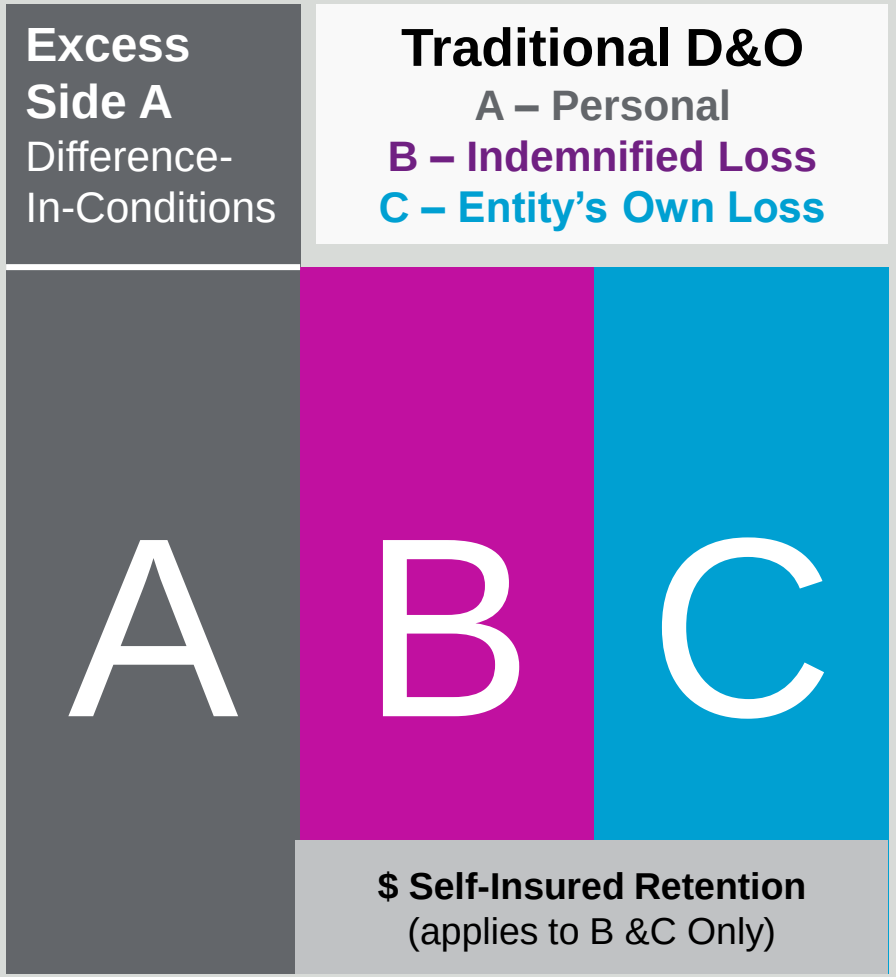
Directors and Officers Liability – today's and tomorrow's insurance opportunities and challenges

1. What should we expect from carriers this year in response to our hard market and this difficult environment?
   - Pricing
   - Capacity
   - Terms

2. How should we prepare for this year's renewal? What information is most important to carriers?

3. Capacity—What if I cannot get all the coverage I want or have? What are my options?

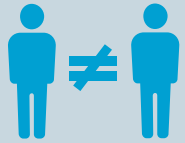
4. Cost v. Value—While prices for D&O are going up significantly, D&O is still a critical, valuable coverage.



Employment Practices Liability – Exposures

Discrimination

- Title VII
- Americans with Disabilities Act (ADA)
- Age Discrimination in Employment Act (ADEA)
- Equal Pay Act
- GINA



Retaliation

- Section 7 of the NLRA
- In response to requesting leave or an accommodation
- In response to raising concerns of workplace safety

Privacy

- Questioning employees about their personal health, health history or family health history
- Test and temperature taking

Wage and hour

- Difficulty tracking time when working remotely
- Additional requirements (temperature taking and putting on PPE) – compensable?
- Duties test – are exempt workers doing non-exempt work now?

Employment Practices Liability – Insurance

Takeaway: EPL underwriters are focused on COVID-19's impact

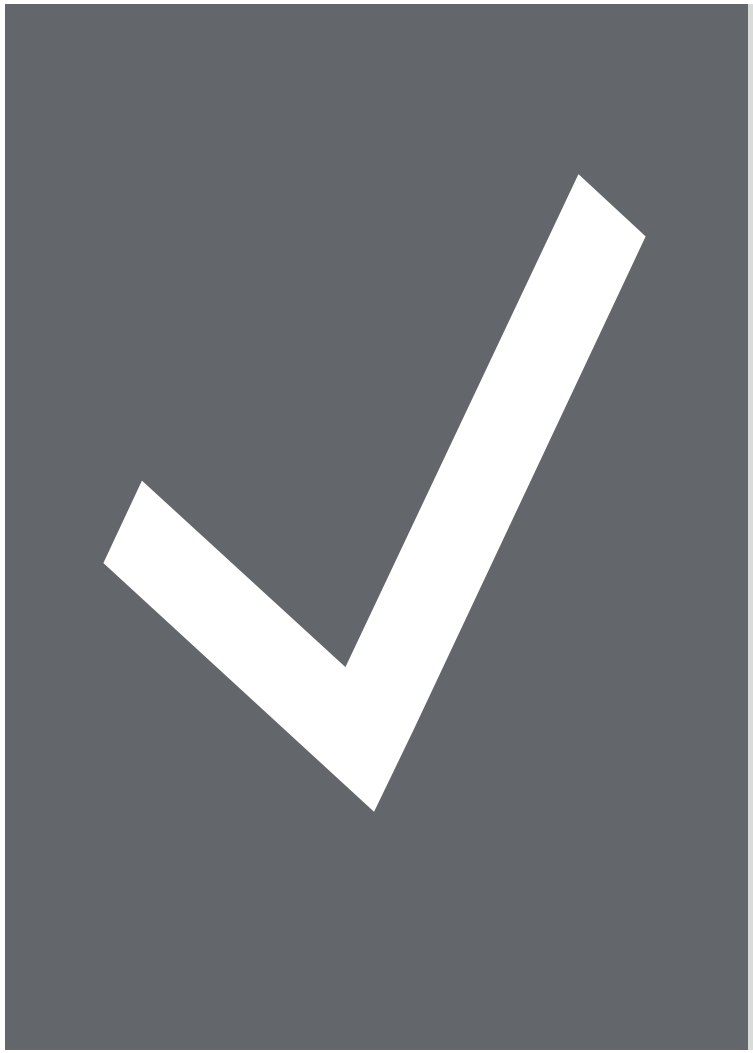
Market update

- Rate increases across the board
- Continued pressure on retention, expect separate retentions for . . .
  - California
  - High wage earners
- Cutting back of limits/capacity
- Some pull-back on coverage
- Most challenged sectors:
  - Retail
  - Hospitality
  - Healthcare

Underwriting areas of inquiry

- Advise how the company is managing the COVID-19 impact on business
- RIFs, layoffs, furloughs, or closure of business locations – number of employees impacted
- Any plans for new hiring?
- Company's timekeeping and Wage & Hour policies and procedures for non-exempt employees
- Financial liquidity
- Return to workplace/reopening plans

Employment Practices Liability – Best practices



- ✓ Follow federal and local laws about when to open the workplace
- ✓ Determine order of employees returning to work
- ✓ Develop (or update) personnel policies
  - Remote working policies
  - Protocols for employees returning to work
  - Workplace safety protocols
  - COVID-19 leave policies and procedures for requesting and obtaining leave
  - Accommodation requests
- ✓ Provide COVID-19 specific manager training
- ✓ Recommit to I&D efforts
- ✓ Communicate effectively with the workforce

Cyber Insurance

Quick refresher

What is "Cyber Liability Insurance?"

- A risk transfer solution for businesses to protect themselves from the financial impact of cyber threats that could jeopardize their business operations, financial success and sustainability.
- It is a crucial part of any holistic approach to combat an organization's cyber risk.
- People + Capital + Technology

Why Do I need Cyber Liability Insurance?

- Immediate response to First and Third party incidents.
- Coverage solutions address specific cyber exposures across different industries, blending: crime, property, extortion and general liability.

Sources of Cyber Liabilities?

- People – 63% of our claims data is attributable to the human element.
- Rogue Nations
- External bad actors

Insurance Coverages Overview

The cyber insurance market continues to evolve and adapt

Breach Response / Event Management	First Party – Costs associated with Legal/forensics, PR, notification to affected individuals, call-center services, identity theft restoration, data reconstruction or credit monitoring.
Business / Network Interruption	First Party – Payment for loss of income, extra expense, claims preparation costs arising out of network security breach or system failure. Extends to outsourced provider networks.
Cyber Extortion / Ransomware	First Party - Covers extortion payments and expenses to investigate a security threat to release or refuse to unencrypt sensitive information or to bring down a network unless a ransom is paid. Coverage extends to payments made via traditional and non-traditional currencies such as Bitcoin.
Social Engineering	First Party - Money and securities transferred by an insured to an impostor from the insured's good faith reliance upon a received email or instruction that appears to be from a legitimate source.
Regulatory Penalties	First Party - Regulatory fines assessed, and investigative costs following a covered data breach.
Network Security / Privacy Liability	Coverage for indemnity and defense costs for third party claims and regulatory actions alleging a security failure or privacy event. • Usually includes coverage for PCI fines, expenses, and costs
Media Liability	Coverage for indemnity and defense costs for third party claims alleging media wrongful acts such as defamation, disparagement, and copyright/trademark infringement in the dissemination of internet content and media.

Cyber Impacts

Ransomware

- The explosion of ransomware losses in 2019 and into 2020 has had a direct impact on premiums and capacity.
- Ransomware losses have jumped from $500,000 or less per loss to $1,000,000+ per loss.
- As frequency and severity continue to mount, carriers have been reevaluating their primary positions.

$1M	**Typical ransomware loss in 2019** ***We have seen ransomware demands as high as $25M**
$4M	***Average cost of a data breach in 2019, a 12% increase over the past 5 years***
63%	**Cyber losses attributable to the human element**

COVID-19

- An increasing number of malicious cyber actors have looked to exploit the current COVID-19 pandemic for their own objectives.
- Global agencies have detected heightened nefarious cyber activity which has led to increased cyber threats to individuals and businesses.
- In particular, the surge in home/remote working has increased usage of potentially vulnerable services, such as Virtual Private Networks (VPN) and home WiFi networks; malicious actors know this and are actively looking to capitalize.
- Advanced Persistent Threat (APT) groups are known to be targeting individuals, small and medium businesses as well as large organizations with predominantly Social Engineering attack techniques that once again look to capitalize on the global COVID-19 pandemic.
- Heightened Email Based Attack campaigns (such as Phishing) and increased Smishing (SMS based attacks) are common place.
- Individuals and organizations alike must apply the enhanced due care and attention to the cyber security of their workforce, their data, systems, networks and devices through this troubling time.

Cyber Insurance

Takeaways/Trends

Market update

- Rate increases across primary and excess markets +10% to +15%.
- Long term uncertainty around BI/Ransomware
- Business interruption/system failure continues to be an area of concern for underwriters.
- Heavily exposed industry classes, such as aviation, manufacturing and transportation, healthcare, and retail have seen increased underwriting scrutiny.
- While coverage remains available, certain industries face significant premium increases.
- Capacity constraints

Renewal & Underwriting

- Carriers are more frequently utilizing outside third parties to assist them with underwriting diligence.
- Ransomware supplemental applications have become the norm.
- COVID-19 questions
- This requires more detailed discussions with CIO's, CISO's and others within the organization who can respond appropriately.
- Start renewal discussions early
  - Establish renewal strategy
  - Utilize analytical tools – Cyber Quantified/Benchmarking

Solving claims issues in a time of crisis and hardening market

Claims challenges and opportunities

1. Has COVID-19 and the hard market impacted how claims are handled?
2. How can brokers help maximize insurance recoveries?
3. Forecast? What's ahead?
4. Notice of Circumstances
5. Timely defense cost reimbursement to support cash flow

Questions

Upcoming events:

June 30: Distressed Organizations

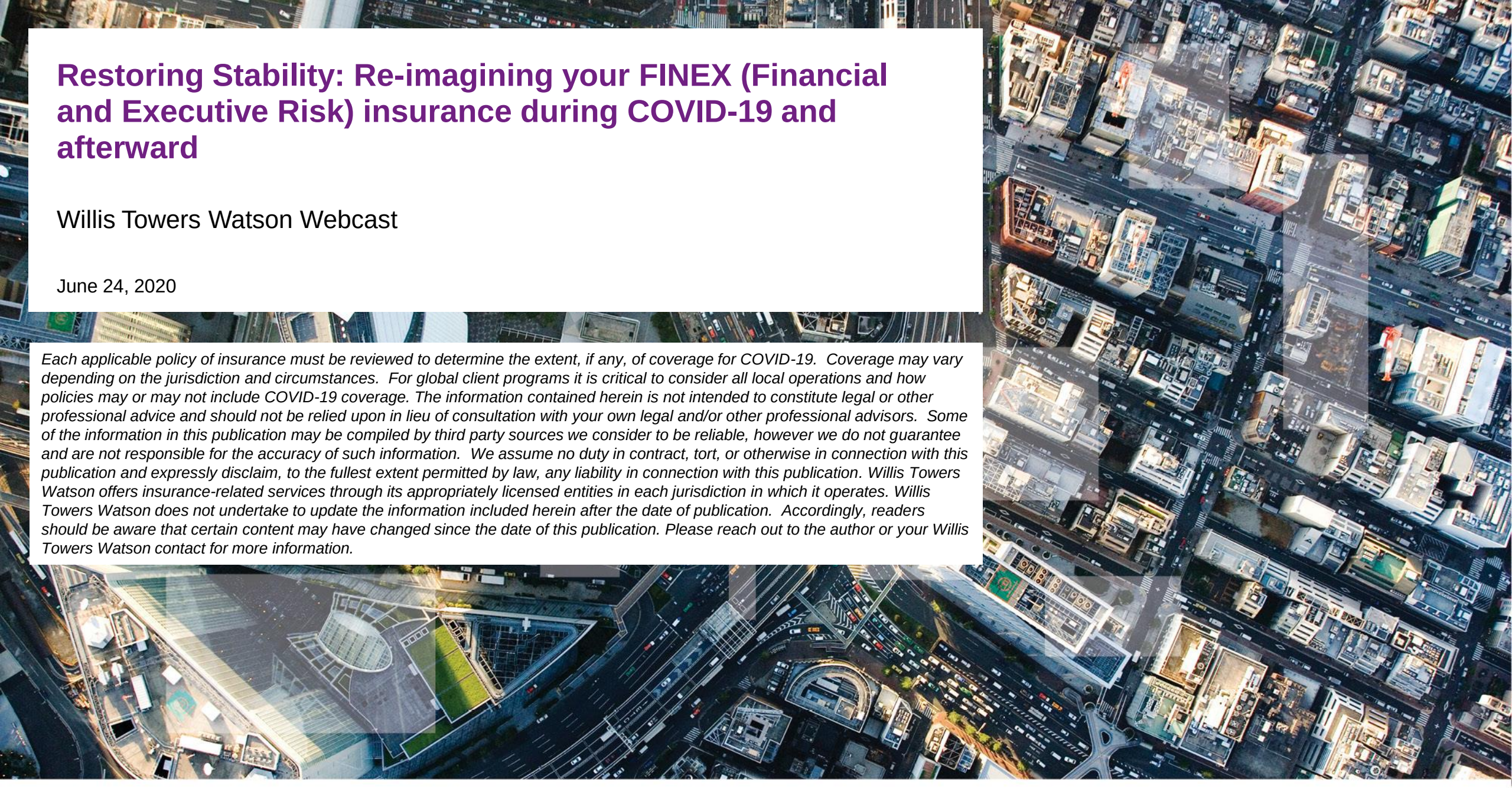
July 9: Dealing with a Difficult Umbrella Market

Register for future events and access past recordings on willistowerswatson.com

Restoring Stability: Re-imagining your FINEX (Financial and Executive Risk) insurance during COVID-19 and afterward

Willis Towers Watson Webcast

June 24, 2020



Each applicable policy of insurance must be reviewed to determine the extent, if any, of coverage for COVID-19. Coverage may vary depending on the jurisdiction and circumstances. For global client programs it is critical to consider all local operations and how policies may or may not include COVID-19 coverage. The information contained herein is not intended to constitute legal or other professional advice and should not be relied upon in lieu of consultation with your own legal and/or other professional advisors. Some of the information in this publication may be compiled by third party sources we consider to be reliable, however we do not guarantee and are not responsible for the accuracy of such information. We assume no duty in contract, tort, or otherwise in connection with this publication and expressly disclaim, to the fullest extent permitted by law, any liability in connection with this publication. Willis Towers Watson offers insurance-related services through its appropriately licensed entities in each jurisdiction in which it operates. Willis Towers Watson does not undertake to update the information included herein after the date of publication. Accordingly, readers should be aware that certain content may have changed since the date of this publication. Please reach out to the author or your Willis Towers Watson contact for more information.

Willis Towers Watson