Loss Executives Association
P.O. Box 37 ♦ Tenafly, NJ 07670 ♦ Phone: 201-569-3346
Email: info@lossexecutives.com

LEA 2016 YOUNG PROFESSIONALS SEMINAR
November 7, 2019

St. John's University School of Risk Management
101 Astor Place ♦ New York, NY
(Between 3rd & 4th Avenues)

Program Agenda

9:00 – 10:00 am **Registration/Continental Breakfast**

10:00 – 10:10 am **Welcome**
Brandon Sweitzer, Dean St. John's University School of Risk Management
Paul Aviles, LEA President

9:15 – 10:15 am **Superman**

Presenter: ***Mr. Tony Canas, Jacobson Group.***

a. Why Millennials are Different

b. Understanding the Demography or the Overall Economy

c. How the Insurance Industry's Demographic Exacerbate the Problem

d. The Importance of Culture

e. The Effect of the InsurTech Revolution

f. Solutions to Engage Millennials

g. Preparing for Gen Z

11:00 – 11:30 am **Cyber Attacks & Risks**

Presenter: ***Ms. Lori Hayes, Thornton Tomasetti***

a. Cybersecurity Foundations 101
   i. What is Cybersecurity?
   ii. Types of Cyber Attacks
   iii. Targets of Cyber Attacks
   iv. Who is the Hacker? (Demonstration)

b. Cybersecurity - Cultural Norms
   i. Cyber-attack – Threats, Vulnerabilities, & Risks
   ii. Privacy

c. Cybersecurity – What are the real threats?
    i. Hacking
    ii. Phishing/Vishing
    iii. Ransomware Attacks
    iv. Third Party/Insider Threat

11:30 – 12:20 pm **Cyber Risk Insurance: The New Reality**

Presenter: ***Professor Mark Browne***
St. John's University School of Risk Management

a. Elements of Cyber Risk
    i. Definition of Cyber Risk
    ii. Types of Cyber Risk
        1. First-party vs. Third Party Exposure
        2. Incident Types

b. Discussion of Some Major Cyber Losses
    i. Sony 2011
    ii. Ashley Madison 2015
    iii. Equifax 2017
    iv. Under Armour 2018

c. Evolution of Cyber Risk
    i. Generation 1 (1980s): Initial Viruses
    ii. Generation 2 (1990s): Initial Network Attacks
    iii. Generation 3 (2000s): App Targeted Attacks
    iv. Generation 4 (2010s): Advanced Malware
    v. Generation 5 (2017+): Large-scale Attacks

d. Insurability of Cyber Risk
    i. Characteristics of insurable risks
    ii. Cyber insurance products
    iii. Cyber insurance marketplace

12:20 – 1:20 pm **Lunch**

1:20 – 1:50 pm **Cyber Law and Loss Scenario**

Presenter: ***Mr. Cos Suriano, Mound Cotton Wollan & Greengrass***

a. Current Legislative Mandates

b. First Party Cyber

c. New Legal Theories

Loss Scenario Hypothetical Loss Scenario

1:50 – 2:20 pm **Adjustment Challenges**

Presenter: ***Mr. Kurt Chapin, Chubb***
Mr. Joe Roskop, McLarens

a. Ask audience some obstacles that the adjuster themselves may face
    i. What do the policy limits say?
    ii. Who will the adjustment team be?
    iii. Who is the lead UW who will be approving/ directing the adjustment team?

b. Discuss why these initial tasks are important to begin the investigation
    i. Need adjustment team with experience in these matters
    ii. Need counsel who has knowledge of the situation and what may or may not be afforded coverage
    iii. Make sure you are on the same page as the lead UW as they will be directing you on how to proceed and what is needed

c. Discuss obstacles that may arise during the investigation
    i. Could this have been avoided?
    ii. Are there coverage issues?
        - Are there potential exclusions?
        - If so, what type of ensuing loss language to the exclusions contain and how may they impact claims for water and fire?
        - Does the insured have a cyber policy and, if not, what issues do you see for a property policy related to:
            - Inoperable electronic network; is this physical loss?
            - How would the policy respond to the ransom? Could this be covered as an extra expense? Would business income coverages apply to all losses or just some?
    iii. Are there any additional long-term effects?
    iv. Can the Insured get up and running again?

2:20 – 2:50 pm **Property Damage: Distribution System, IT, Building**

Presenter: ***Mr. Scott Armstrong, J.S. Held***

a. IT (Cyber Crime Recovery)
    i. Assessment of IT Systems Impact
    ii. Recovery Solutions
    iii. Disaster Recovery Centers / Backup Sites

b. Property Damage Assessment
    i. Formulating Team of Experts
    ii. Protocol for Equipment Damage Assessment
    iii. Ion Chromatography / Microscopy Analysis
    iv. Inventory / Configuration Validation
    v. Replacement Cost Valuation

c. Restoring Production Capabilities

2:50 – 3:10 pm **Break**

3:10 – 3:40 pm **Production Impact & Business Interruption**

Presenter: ***Mr. Michael Castillo, Meaden***

a. What is Business Interruption?
    i. Key Concepts
        1. Actual Loss Sustained
        2. Business Income
        3. Period of Restoration
        4. Extended Period of Indemnity
        5. Extra Expenses

b. Cyber BI Coverage yesterday, today & tomorrow
    i. Example of Cyber Losses
        1. Department Store Credit Card database hacked
            a. No physical damage
            b. No BI exposure to the department store
        2. Assisted Living Facility
            a. Physical damage to server
            b. Hacking of personal data
            c. Cost to restore data
            d. Reputational Harm – BI
        3. Future Loss at XYZ Company
            a. Complete shutdown of production & distribution facility
            b. Reputational Harm - BI
            c. BI & EE
            d. First & Third-Party Liability

c. Batchko Inc. – Online Retailer

i. Operations of all worldwide distribution centers cease…
   a. Effects on business…

ii. Fire at Distribution Centers
   a. Stock Loss…

iii. Lost Sales / Shipping

iv. Sales Value of Stock

v. Receipt of New Inventory

b. Temporary Locations

i. Forecasting Lost Sales
   a. Historical Sales
   b. Industry Trends

3:40 – 4:10 pm **Questions Presented by Loss Scenario**

Presenters: ***Mr. Paul Carnovale, Aegis***
Mr. Nigel Shepherd, Aegis

a. Which policy(ies) apply to the loss?
b. Would this be considered one or multiple occurrences? Would multiple deductibles apply?
c. Which policy would cover any tangible property losses (laptops, etc.) and which would cover any intangible losses (loss of electronic data)
d. Would the hostile Act/terrorism/war exclusion apply?
e. If the company has a cyber liability policy, what assistance would the cyber carrier provide to mitigate these claims?
f. Is there a concurrent causation (the cyber attack caused the fire, which in turn caused property damage) issue?
g. Did the Executive Vice President prejudice the rights of the insurers by doing nothing? Did his inaction create the event by not mitigating the potential loss and is he required to do so?

4:10 – 4:45pm **Lessons Learned**

Presenters: ***Mr. Ray Mattia, AIG***
Mr. Paul Aviles, AWAC

4:45 – 5:30 pm **Cocktails**

LEA BOARD OF DIRECTOR

OFFICERS

President
Paul Aviles
Allied World Assurance Company (USA) Inc.

Vice President
Raymond Mattia
AIG

Treasurer
Thomas Casson
AIG

Secretary
Jose Morgatoff
Zurich N.A.

Immediate Past President
Jean L. Broderick, ARe
XL Catlin
AXA XL, a division of AXA

BOARD OF DIRECTORS

Paul Carnovale
Chubb

Marisa Jelicks
Liberty Mutual Insurance

Jim Jezewski
Starr Technical Risks Agency, Inc.

Michael Koski
RSUI Group Inc.

Nigel Shepherd
Aegis Security Insurance Company

Brooke Shultz
Mutual Boiler Re
Member of the FM Global Group

Maxine E. Walker
FM Global

Steven Yeo
Lancashire Insurance Company (UK) Limited

Counsel
Costantino Suriano, Esq.
Mound Cotton Wollan & Greengrass

Board Consultant
Scott Armstrong
Werlinger & Associates, Inc.

Board Consultant/Accountant
Gerald W. Warshaw
Matson Driscoll & Damico LLP

CE Coordinator
Louis D. Magnan, CPA
Magnan Graizzaro & Asociaste CPAs, LLC

Membership Chair & Web Master
Margaret A. Reilly
Edward R. Reilly & Co., Inc.

Meeting Coordinator/Event Planner
Maria Sclafani
The Beaumont Group, Inc.