SOCIETY OF ACTUARIES®

2019 ANNUAL MEETING & EXHIBIT

October 27-30
Toronto, Canada

Session 099: Managing Cyber Risk

SOA Antitrust Compliance Guidelines
SOA Presentation Disclaimer

Cyber Risk Panel

Society of Actuaries

2019 Annual Meeting & Exhibit

Toronto

OCTOBER 29, 2019

Themes

Maersk's experience highlights key themes in cyber risk

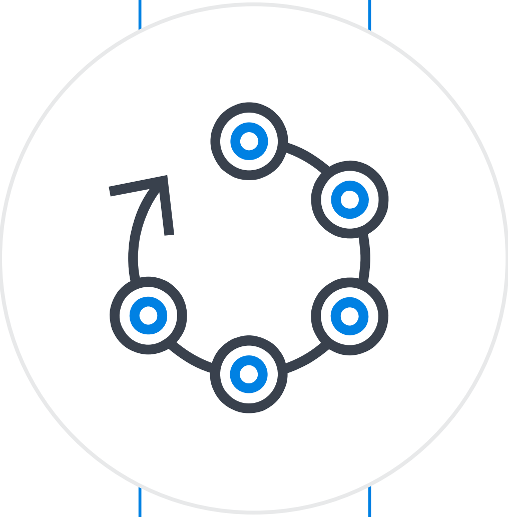
Repeat issues

Normalcy bias
Extreme events are underestimated while it is believed systems will function as assumed

Virus propagation velocity
The virus spread in hours if not minutes

Cascading failure
The virus propagated throughout Ukraine and spread globally

Recovery serendipity
Maersk was only able to recover in 10 days due to a blackout in Ghana



Emerging issues

Attack attribution
State actors possess the greatest cyber capabilities but it is difficult to prove who is responsible

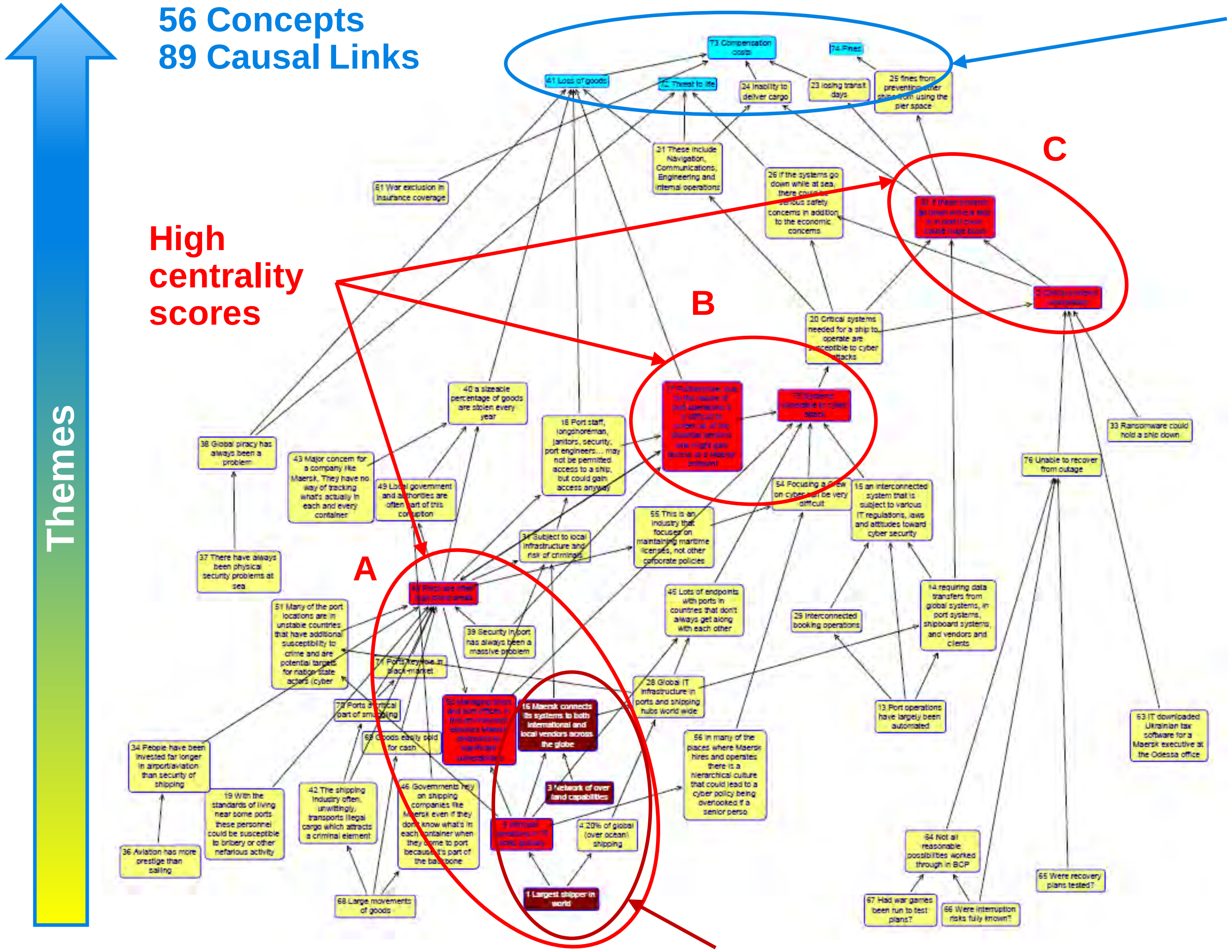
Insurance coverage
NotPetya highlights the problem of "silent cyber" or non-affirmative risk and its impact on accumulation risk

War Exclusion
Zurich denied Mondelez's $100 MM claim, citing NotPetya as an act of war; the case is pending in court

Law of unintended consequences
It is doubtful that Maersk was a deliberate target of NotPetya

Visualizing Maersk’s exposure

A cognitive map was created to highlight the critical paths to Maersk’s NotPetya incident


Themes
73 Compensation costs
74 Fines
41 Loss of goods
72 Threat to life
24 Inability to deliver cargo
23 losing transit days
25 fines from preventing other ships from using the pier space
21 These include Navigation, Communications, Engineering and internal operations
26 If the systems go down while at sea, there could be serious safety concerns in addition to the economic concerns
61 War exclusion in insurance coverage
22 If these systems go down while a ship is in port it could cause huge costs
2 Critical systems unavailable
20 Critical systems needed for a ship to operate are susceptible to cyber attacks
17 Furthermore, due to the nature of port operations it is difficult to screen all of the potential persons who might gain access to a Maersk endpoint
75 Systems vulnerable to cyber attack
33 Ransomware could hold a ship down
76 Unable to recover from outage
40 a sizeable percentage of goods are stolen every year
18 Port staff, longshoreman, janitors, security, port engineers... may not be permitted access to a ship, but could gain access anyway
38 Global piracy has always been a problem
43 Major concern for a company like Maersk. They have no way of tracking whats actually in each and every container
49 Local government and authorities are often part of this corruption
54 Focusing a crew on cyber can be very difficult
15 an interconnected system that is subject to various IT regulations, laws and attitudes toward cyber security
55 This is an industry that focuses on maintaining maritime licenses, not other corporate policies
34 Subject to local infrastructure and risk of criminals
37 There have always been physical security problems at sea
48 Ports are often high crime areas
45 Lots of endpoints with ports in countries that don't always get along with each other
29 Interconnected booking operations
14 requiring data transfers from global systems, in port systems, shipboard systems, and vendors and clients
51 Many of the port locations are in unstable countries that have additional susceptibility to crime and are potential targets for nation state actors (cyber
39 Security in port has always been a massive problem
71 Ports keyhole in black-market
28 Global IT infrastructure in ports and shipping hubs world wide
70 Ports a critical part of smuggling
50 Managing ships and port offices in this environment exposes Maersk endpoints to significant vulnerabilities
16 Maersk connects its systems to both international and local vendors across the globe
13 Port operations have largely been automated
63 IT downloaded Ukrainian tax software for a Maersk executive at the Odessa office
69 Goods easily sold for cash
56 In many of the places where Maersk hires and operates there is a hierarchical culture that could lead to a cyber policy being overlooked if a senior perso
34 People have been invested far longer in airport/aviation than security of shipping
19 With the standards of living near some ports these personnel could be susceptible to bribery or other nefarious activity
42 The shipping industry often, unwittingly, transports illegal cargo which attracts a criminal element
46 Governments rely on shipping companies like Maersk even if they don't know what's in each container when they come to port because it's part of the backbone
3 Network of over land capabilities
5 Principal operations in 76 ports globally
4 20% of global (over ocean) shipping
36 Aviation has more prestige than sailing
1 Largest shipper in world
64 Not all reasonable possibilities worked through in BCP
65 Were recovery plans tested?
68 Large movements of goods
67 Had war games been run to test plans?
66 Were interruption risks fully known?
A
B
C

56 Concepts
89 Causal Links

High centrality scores

Drivers which lead to the highly connected nodes

Outcomes

Compensation Costs, Loss of Goods, Threat to Life, Fines

Drivers

1 Largest shipper in world

3 Network of overland capabilities worldwide

16 Maersk connects its systems to both international and local vendors across the globe world

Group A

5 Principal operations in 76 ports globally

48 Ports are often high crime areas

50 Managing ships and port offices in this environment exposes Maersk endpoints to significant vulnerabilities

Group B

17 Due to the nature of port operations it is difficult to screen all of the potential persons who might gain access to an endpoint

75 Systems vulnerable to cyber attack

Group C

2 Critical systems unavailable

22 If these systems go down while a ship is in port it could cause huge costs

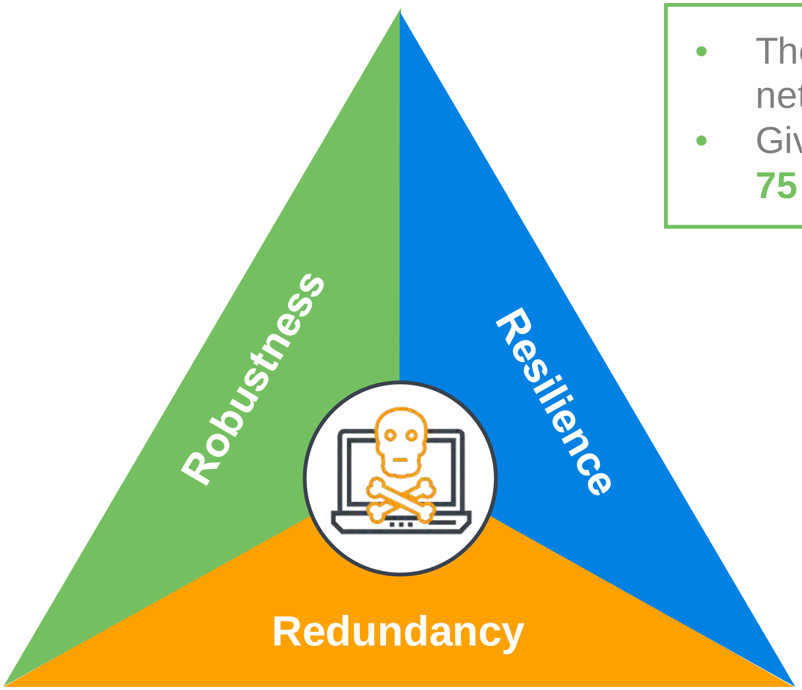
NotPetya highlights the “3 R’s” of risk management

Causal modeling incorporates the importance of network science in managing risk

1. **Can my system maintain its basic functions under duress?**

2. **Can my system adapt to shocks by changing its operations without losing function? How dynamic are my core activities?**

3. **Are there parallel components and functions that can replace other components and functions that fail under duress?**



- The **interconnectedness** of Maersk’s shipping network aggravated the impact of the attack
- Given these dependencies, Maersk was **disabled in 75 out of 76 ports**

- **BCP/DR plans appeared to fail** and did not imagine an attack with aggressive propagation
- **IT was overwhelmed** by the attack
- Without the **accidental backup from Accra**, Maersk would have suffered greater 1st, 2nd and 3rd order losses

- Both **digital and analog redundancy** (paper manifests, etc.) was lacking
- Employees used **ad hoc tools** such as Excel and WhatsApp to maintain minimal operations

Getting to the “big picture”

It is doubtful assessments, frameworks or existing data would have avoided Maersk’s outcome

Standard cyber security approaches

Control Frameworks

- Detailed self-assessments based on checklists endorsed by industries and/or regulators
- Data inputs are scored on an ordinal scale (1 - 5)
- Results are transposed to a risk matrix using a qualitative rating, e.g., HML (High/Medium/Low) or RAG (Red/Amber/Green)

Stand Alone Metrics

- Individual metrics that describe specific programs or controls (Patch timing, dwell time, CMBD…)
- Describes specific controls and programs as isolated entities
- Metrics often describe performance as opposed to risk

“Red Team” Exercises (aka “Ethical Hacking”)

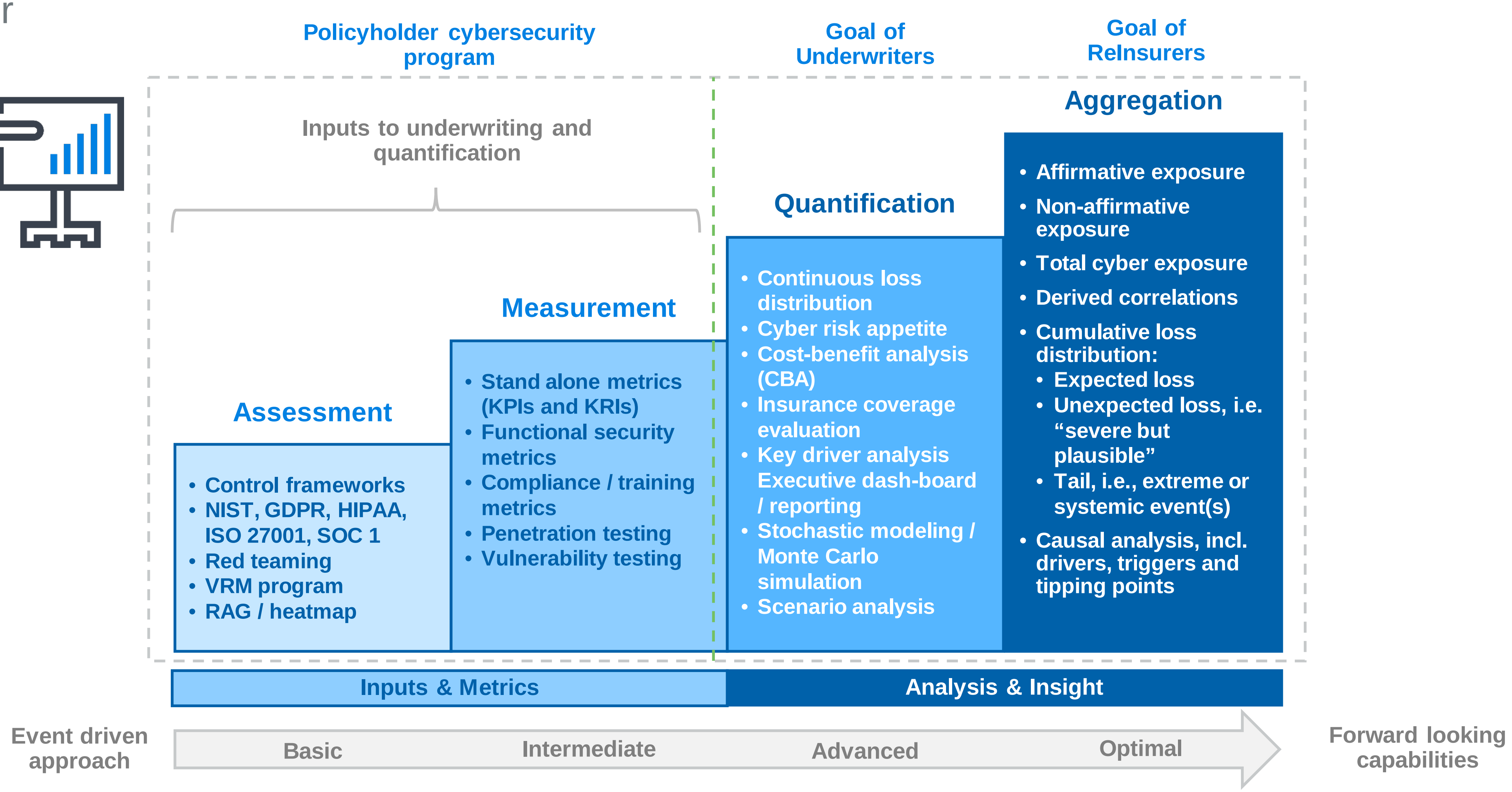
- Uses tactics that are assumed to be similar to leading threats
- Illustrates the human and technical vulnerabilities that could lead to a cyber event
- Produces a detailed path for a specific threat

Point Score

- Aggregation of controls assessments and stand alone metrics into a single point score
- Created by either third party propriety aggregation tools or internal point values assignments
- Gives a single measurement for cyber risk

Cyber risk maturity

To effectively aggregate exposure, [re]insurers must be among the most mature in evaluating cyber



Policyholder cybersecurity program

Goal of Underwriters

Goal of ReInsurers

Inputs to underwriting and quantification

Assessment

- Control frameworks
- NIST, GDPR, HIPAA, ISO 27001, SOC 1
- Red teaming
- VRM program
- RAG / heatmap

Measurement

- Stand alone metrics (KPIs and KRIs)
- Functional security metrics
- Compliance / training metrics
- Penetration testing
- Vulnerability testing

Quantification

- Continuous loss distribution
- Cyber risk appetite
- Cost-benefit analysis (CBA)
- Insurance coverage evaluation
- Key driver analysis Executive dash-board / reporting
- Stochastic modeling / Monte Carlo simulation
- Scenario analysis

Aggregation

- Affirmative exposure
- Non-affirmative exposure
- Total cyber exposure
- Derived correlations
- Cumulative loss distribution:
  - Expected loss
  - Unexpected loss, i.e. “severe but plausible”
  - Tail, i.e., extreme or systemic event(s)
- Causal analysis, incl. drivers, triggers and tipping points

Inputs & Metrics

Analysis & Insight

Event driven approach

Basic

Intermediate

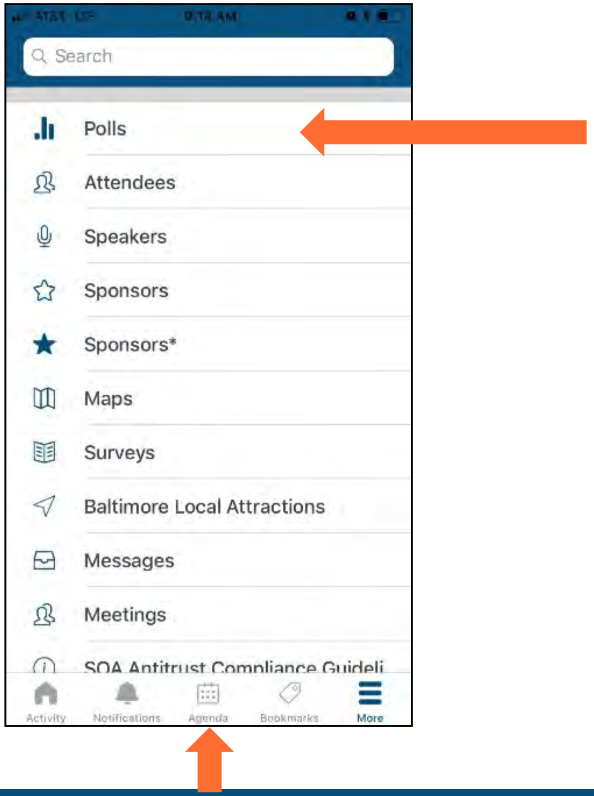
Advanced

Optimal

Forward looking capabilities

To Participate, look for Polls in the SOA Event App or visit annual.cnf.io in your browser

Find The Polls Feature Under **More** In The Event App or Under This Session in the Agenda


Search

Polls

Attendees

Speakers

Sponsors

Sponsors*

Maps

Surveys

Baltimore Local Attractions

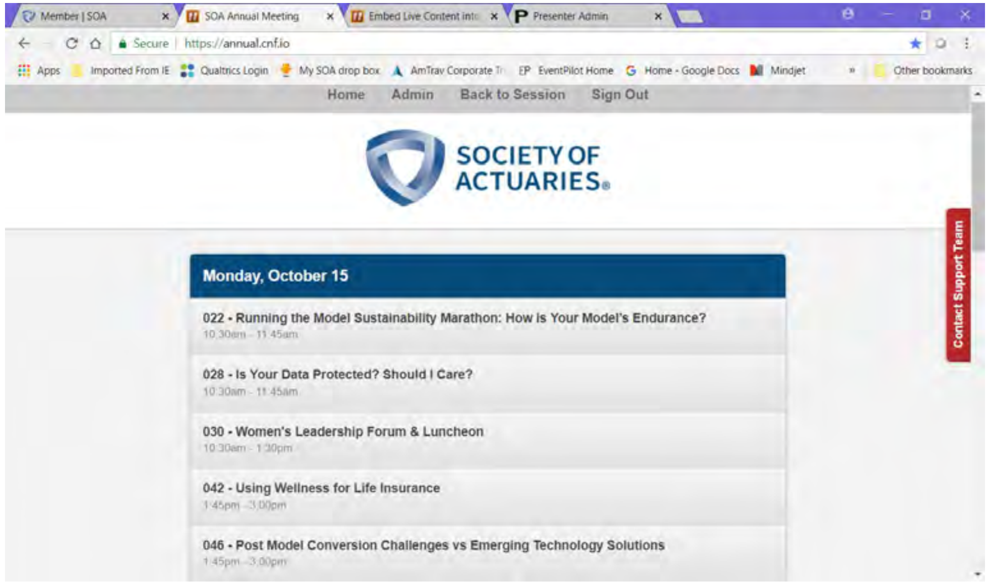
Messages

Meetings

SOA Antitrust Compliance Guideli

or

Type annual.cnf.io In Your Browser



Monday, October 15

022 - Running the Model Sustainability Marathon: How is Your Model's Endurance?
10:30am - 11:45am

028 - Is Your Data Protected? Should I Care?
10:30am - 11:45am

030 - Women's Leadership Forum & Luncheon
10:30am - 1:30pm

042 - Using Wellness for Life Insurance
1:45pm - 3:00pm

046 - Post Model Conversion Challenges vs Emerging Technology Solutions
1:45pm - 3:00pm

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Where do you work?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: What is your role?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: What are your greatest cyber risk concerns? Select all that apply.

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Did your organization have claims due to NotPetya?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Does your company view cyber as a risk or a peril?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Does your claims process for non-cyber policies allow for tracing back to a cyber event as the trigger?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Do your cyber policies include language for excluding hostile acts or war?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Has your company experienced a breach in the past 12 months?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Does your company have regular cybersecurity training, i.e., phishing awareness, etc.?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Do you use a questionnaire to assess a firm's cyber risk before pricing insurance products?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Do you use a diagnostic tool and client data to price cyber insurance products?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Do you have a model that underwrites cyber risk?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: What method do you use?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Does you model capture both affirmative and non-affirmative cyber risk?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Do you have a claims taxonomy to map affirmative vs. non-affirmative cyber risk?

Live Content Slide

When playing as a slideshow, this slide will display live content

Poll: Which of the following do you review when pricing insurance products? Select all that apply.