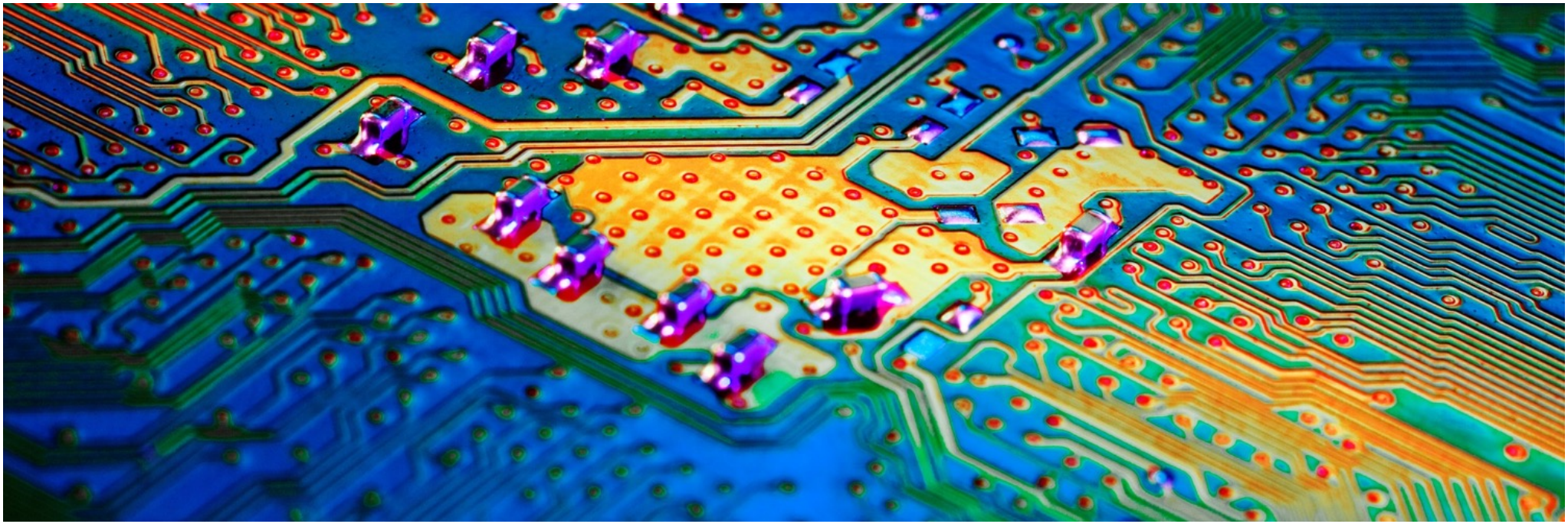


New approaches to modeling silent cyber risk

Jon Laux and Ridhima Kale

GUIDEWIRE CYENCE

AON Empower Results®

Antitrust Notice

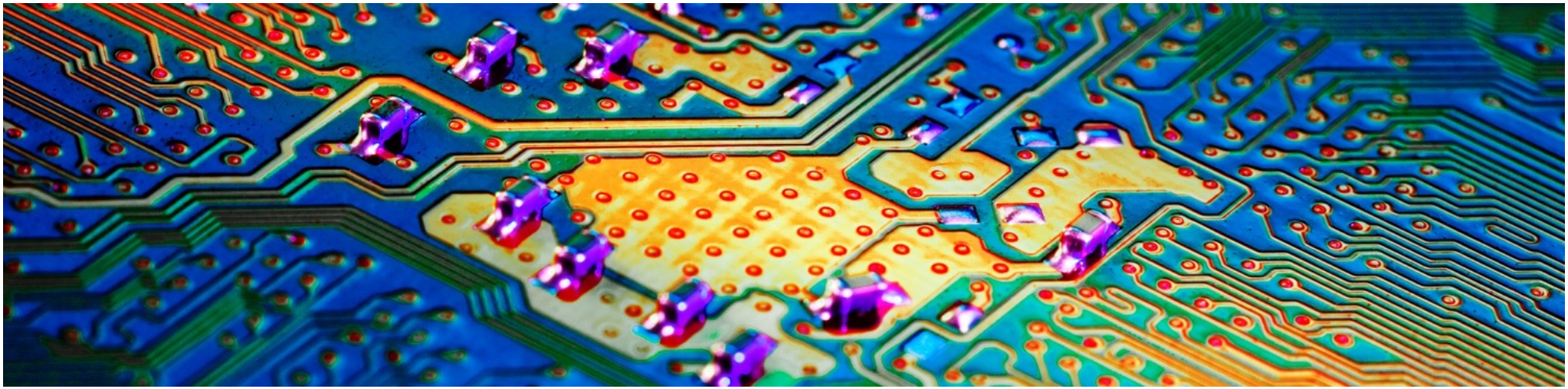
- The Casualty Actuarial Society is committed to adhering strictly to the letter and spirit of the antitrust laws. Seminars conducted under the auspices of the CAS are designed solely to provide a forum for the expression of various points of view on topics described in the programs or agendas for such meetings.
- Under no circumstances shall CAS seminars be used as a means for competing companies or firms to reach any understanding – expressed or implied – that restricts competition or in any way impairs the ability of members to exercise independent business judgment regarding matters affecting competition.
- It is the responsibility of all seminar participants to be aware of antitrust regulations, to prevent any written or verbal discussions that appear to violate these laws, and to adhere in every respect to the CAS antitrust compliance policy.

Agenda

1. What is silent cyber and why is it important?
2. Identifying and quantifying silent cyber risk
3. The future

GUIDEWIRE CYENCE

AON Empower Results®



1. Demystifying “silent” cyber risk

GUIDEWIRE CYENCE

AON Empower Results®

Defining Silent Cyber Risk

Aka “non-affirmative cyber” or “cyber as a peril,” silent cyber risk takes one of two forms:

Unintended Coverage

- Most common meaning of “silent cyber”
- Policy language does not explicitly address cyber risk as a potential cause of loss
- Cyber coverage neither excluded, nor affirmatively granted
- Unanticipated events could create surprise aggregation of claims

Unpriced Coverage

- Cyber risk implicitly accepted, but no premium is allocated or charged for the risk
- Cyberattack is not a covered cause of loss, but could trigger a covered peril / cause of loss
- No adjustment to premium for marginal increase in frequency / severity due to cyber attack risk

GUIDEWIRE CYENCE

AON Empower Results®

Cyber Risk: Impacts and Coverages

		Property	GL	Crime	PL	Cyber
1st Party Privacy / Network Risks	Breach response costs					
	Damage to data					
	Business interruption					
	Contingent BI					
	Extortion or ransom					
3rd Party Privacy / Network Risks	Theft / disclosure of private data					
	Technology E&O					
	Media liability					
	Damage to 3rd party data					
	Regulatory fines & penalties					
Financial Risks	Social engineering					
Physical Risks	Physical damage					
	Bodily injury					

Affirmative

GUIDEWIRE CYENCE

AON Empower Results®

5 Examples of Potential Silent Cyber Risk

German Steel Mill
- Dec 2014
- Physical damage to blast furnaces

Ukraine Power Plant
- Dec 2015
- 225,000 without power for 6 hours

NotPetya
- Jun 2017
- Attack causing widespread wiperware
- Protracted business interruption at many F500 companies

Rye Brook, NY Dam
- Aug 2013
- Compromised SCADA systems

WannaCry
- May 2017
- Mass ransomware attack
- Impacted UK & US hospitals, Nissan, Renault, & others

GUIDEWIRE CYENCE

AON Empower Results®

Regulatory Pressure around Silent Cyber

> *…risks emanating from cyber as a peril, if not managed well, are potentially significant to the viability of the firms involved*
>
> PRA

> *Lloyd's therefore continues to focus on understanding and discouraging non-affirmative ("silent") cyber risks… Firms are expected to assess and manage their products with specific consideration to non-affirmative cyber risk exposures*
>
> Lloyd's of London

> *Insurers that lack cyber underwriting expertise, poorly manage their risk accumulations or fail to recognize loss potential from "silent" cyber exposure in their traditional commercial insurance products could face pressure on earnings, capital or even ratings, if large loss scenarios emerge as the market expands*
>
> Fitch Ratings

GUIDEWIRE CYENCE

AON Empower Results®

Common Silent Cyber Issues Facing Insurers

Silent cyber poses challenges to insurers on a number of fronts. Some of the main challenges are:

Identifying the exposure

- Non-cyber policies not coded to identify cyber exposure
- Legacy policy systems make it burdensome for insurers to update and code policies

Recognizing the perils

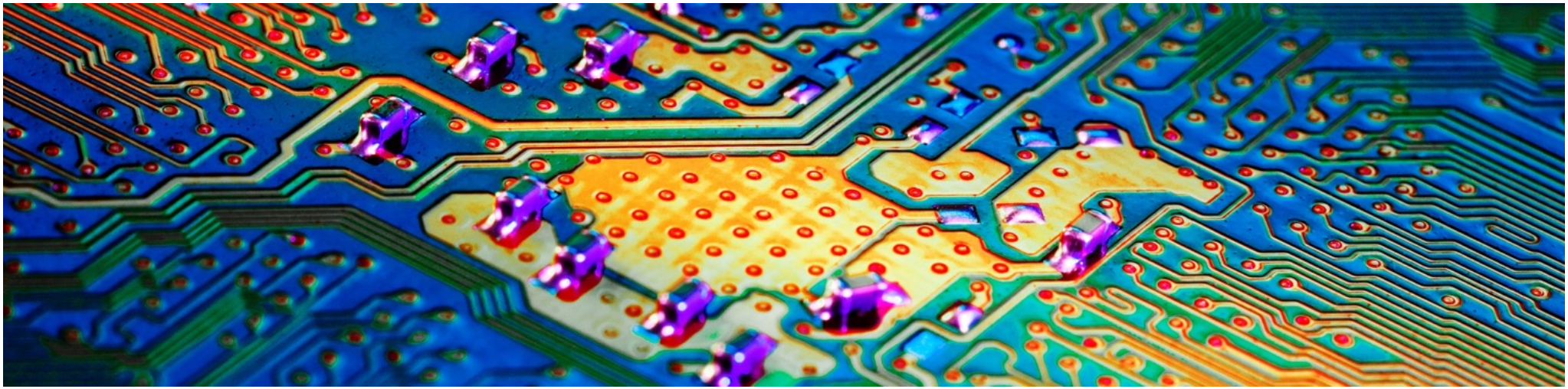
- Policy ambiguity matters when it can be exploited
- Changes in the threat landscape create new ways to exploit old policy wording
- New technologies create potential new risks

Lack of coordination & strategy

- Success requires coordination across many insurance functions
- This is challenging to traditional (re)insurance silos
- Some insurers would prefer to ignore silent cyber or transfer to reinsurers rather than address it

GUIDEWIRE CYENCE

AON Empower Results®



2.1 Identifying “silent” cyber risk

GUIDEWIRE CYENCE

AON Empower Results®

The Process: Assessing, Quantifying & Transferring Silent Cyber Risk

1 Identify lines of business

- Identify LOBs to be included
- Assess reins. exclusions
- Estimate total potential cyber exposure by line

2 Sample original policies

- Sample original policies to see exclusions in place
- Assess strength of exclusions
- Refine the exposure value for each line of business

3 Analyze cyber exposure

- Run current silent cyber scenarios
- Develop custom scenarios that expose your policies

4 Establish long term strategy

- Confirm risk tolerance level
- Benchmark against peer approaches
- Develop a plan to reduce silent cyber exposure over time

5 Silent cyber reinsurance

- Work with markets to find optimal balance between price and structure
- Optimum reinsurance based on more accurate needs assessment

6 Price or exclude cyber

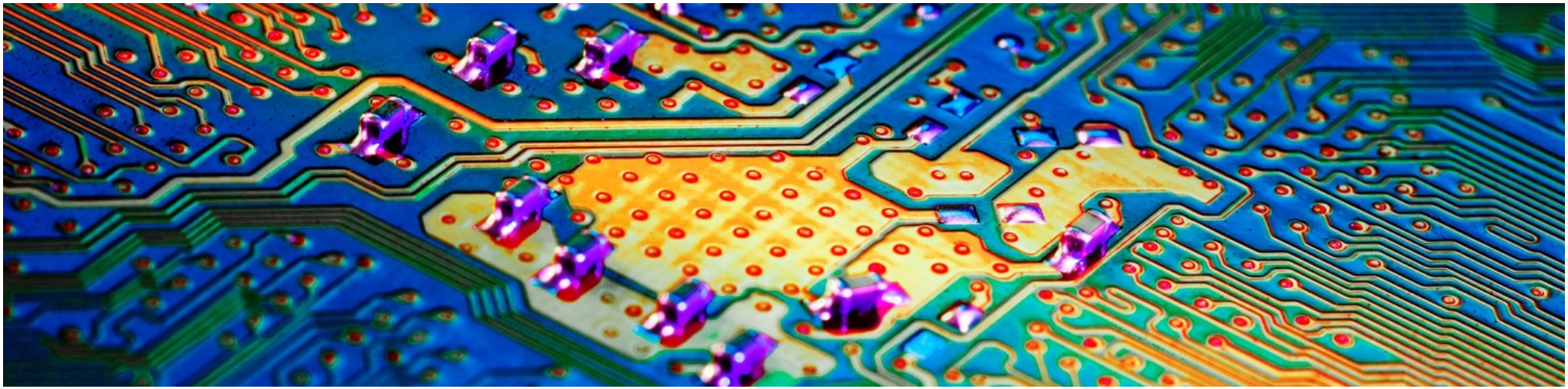
- Underwrite and price for silent cyber across key lines of business
- Coordination between P&C lines and cyber team

7 Affirmative reinsurance

- Establish a program at more competitive price
- Ability to be more versatile (stop loss, QS Agg XL)

GUIDEWIRE CYENCE

AON Empower Results®



2.2 Quantifying “silent” cyber risk

GUIDEWIRE CYENCE

AON Empower Results®

Selecting scenarios to model

Criticality

The event must be relevant and critical to an insurer and its insureds

Data Availability

There should be some historical data that can be used to determine modeling assumptions

Realistic

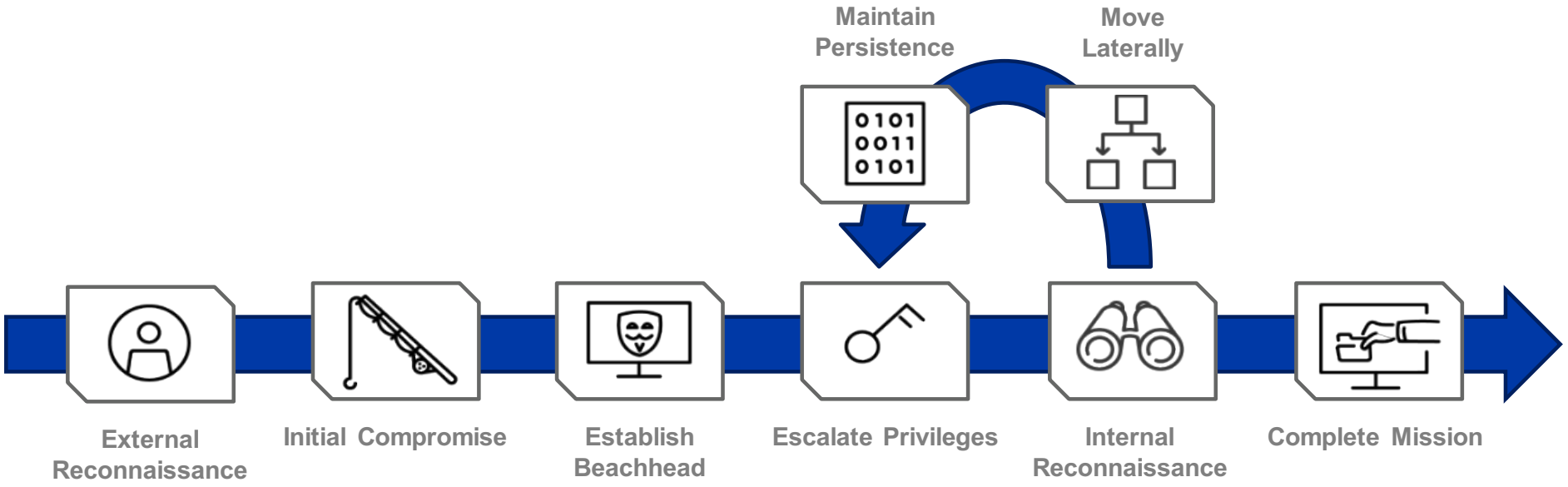
The event must be realistic and have a reasonable likelihood of occurring

Stochastic vs. Deterministic

GUIDEWIRE CYENCE

AON Empower Results®

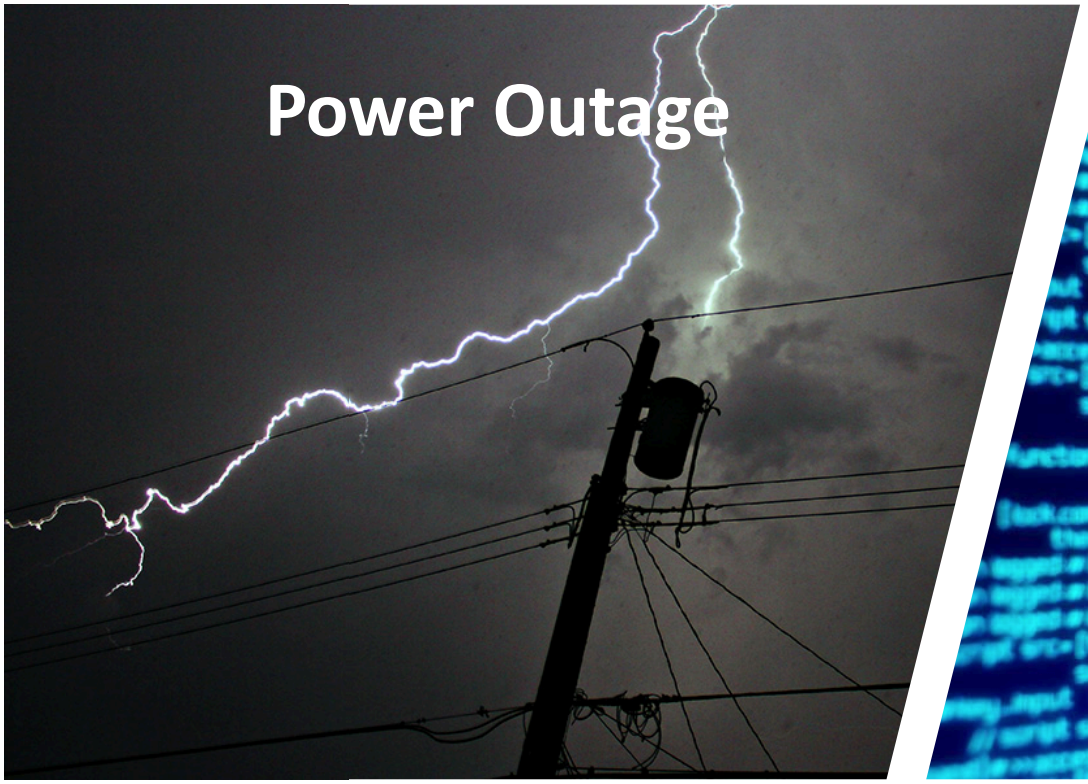
Modeling Unprecedented Events: a Kill Chain Approach



GUIDEWIRE CYENCE

AON Empower Results®

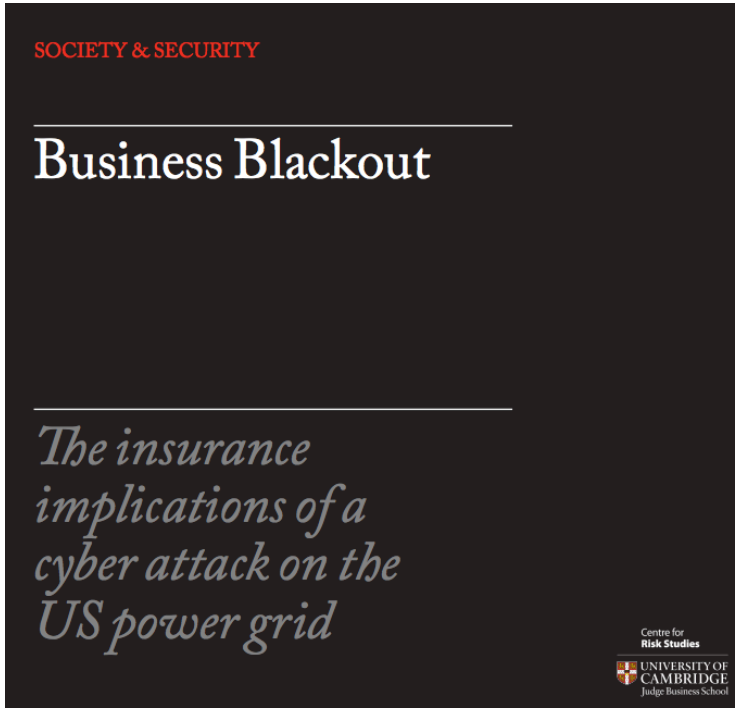
Potential silent cyber scenarios



GUIDEWIRE CYENCE

AON Empower Results®

Power outage



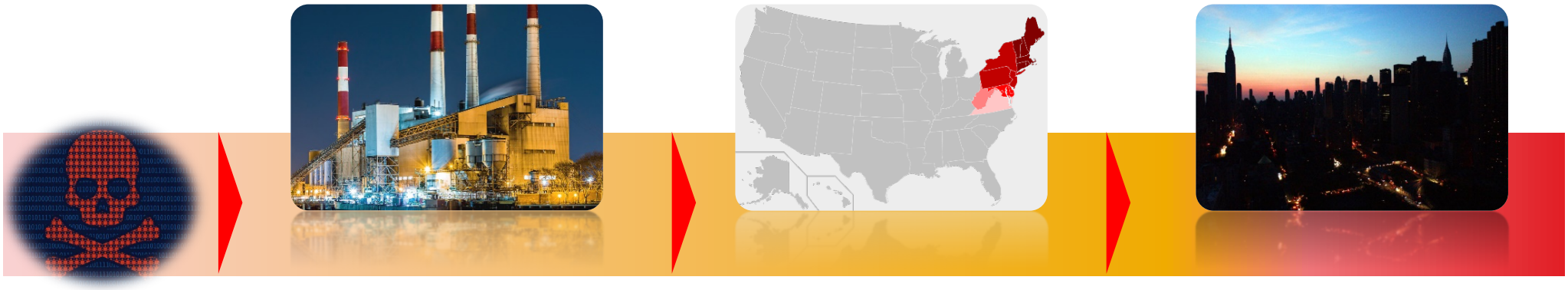
Background:

- As presented in the “Business Blackout”, a cyberattack results in a regional power outage (NE USA)
- Time to recover varies depending on the amount of damage to each power plant.
- Businesses in a region are left without power while repairs can be made.

GUIDEWIRE CYENCE

AON Empower Results®

Power outage



Power generation companies

- Property damage (generators)
- Business interruption, incident response
- Possible litigation

Companies losing power

- Property damage (contents)
- Business interruption & extra expenses

Companies relying on companies losing power

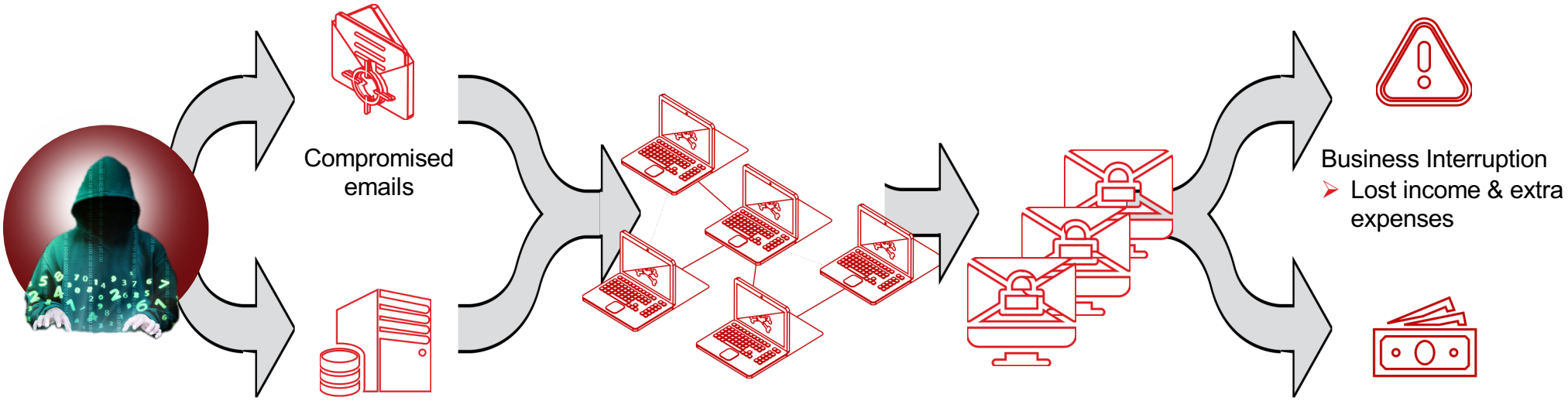
- Indirect business interruption & extra expenses
- Others: Litigation, Homeowners, Specialty, Bodily Injury, WC

GUIDEWIRE CYENCE

AON Empower Results®

Ransomware

Ransomware: Scenario narrative



GUIDEWIRE CYENCE

AON Empower Results®

Future improvements

Current State

Power Outage

- Comprehensive framework to begin quantifying losses
- Availability of deterministic scenario
- Widely recognized critical infrastructure exposure

Ransomware

- Availability of stochastic and deterministic scenario
  - Advanced kill chain methodology
  - Likelihood of an attack
  - Variance in spread of attack
- Identification of companies that are more vulnerable than others
- Ransomware attacks triggering data breach notification requirements

Future Improvement

Power Outage

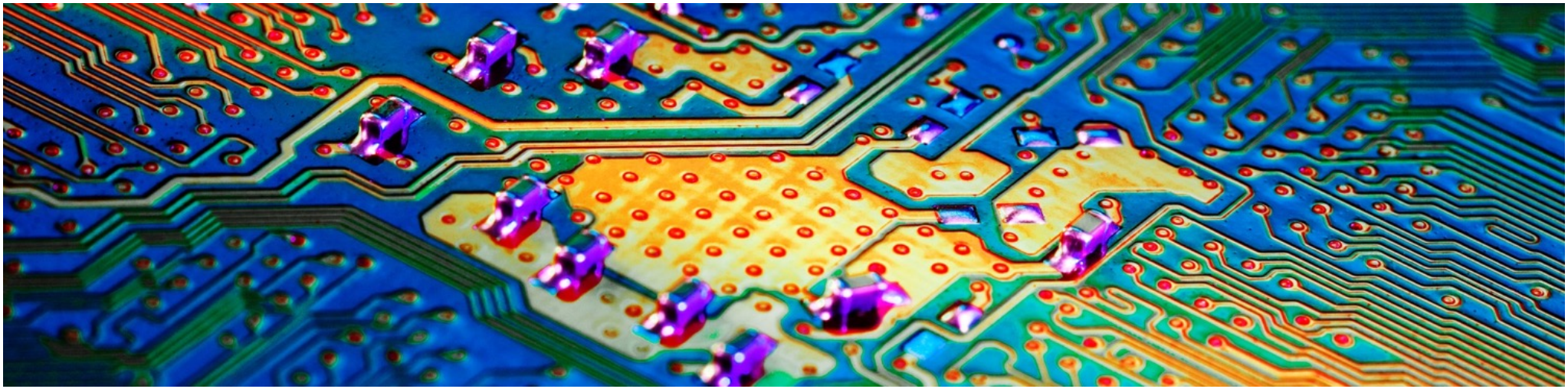
- Likelihood of such an attack
- **Mapping out supply chain**
  - Ideally the insurer has a list of tier 1 suppliers
  - Potential data sources that will map out supply chain (but not perfect)
- **Limited to NE USA**; Additional research for other geographies
- Impact to financial markets
- Technology is constantly evolving and adds complexity to modeling

Ransomware

- **Mapping out supply chain**
  - Ideally the insurer has a list of tier 1 suppliers
  - Potential data sources that will map out supply chain (but not perfect)
- Evolving trend of ransom demands
- Keeping up with new Ransomware variants
- Reporting requirements around Ransomware attacks might evolve

GUIDEWIRE CYENCE

AON Empower Results®



3. The future:
Transferring “silent” cyber, making it affirmative

GUIDEWIRE CYENCE

AON Empower Results®

How have insurers responded

AIG Finalizing Transition to Affirmative Cyber Coverage Across Global Commercial Lines

September 05, 2019 08:30 AM Eastern Daylight Time

NEW YORK--(BUSINESS WIRE)--American International Group, Inc. (NYSE: AIG) today announced that as of January 2020 virtually all of its commercial property and casualty insurance policies will begin affirmatively covering or excluding physical and non-physical cyber exposures, addressing market concerns that traditional commercial insurance policies across the industry – from property to general liability – are often silent about cyber coverage.

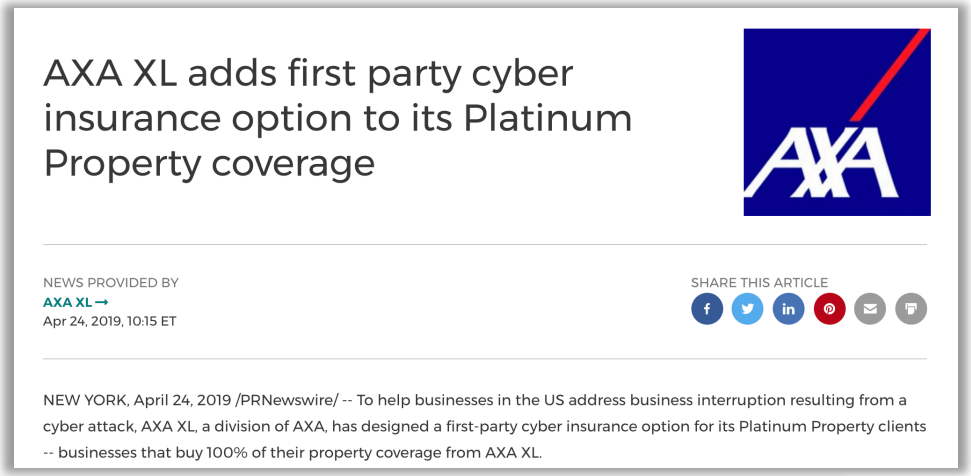
"AIG believes P&C policies globally should be clear about the cyber coverage they provide. For the most part, across the industry, typical P&C policies have not been written to adequately deal with cyber exposure"

Tweet this

For more than 20 years, AIG has offered specific, standalone cyber insurance products that provide a high-level of coverage clarity to clients in the event of a cyber security breach. As the cyber threat has grown in the last five years, AIG has been drawing on that expertise to provide more holistic cyber coverage for clients across standard commercial insurance lines and to incorporate affirmative cyber coverage into traditional P&C policies on a product-by-product basis.

"AIG believes P&C policies globally should be clear about the cyber coverage they provide. For the most part, across the industry, typical P&C policies have not been written to adequately dea

exposure," said Tracie Grella, Global Head of Cyber Insurance. "As we shift to affirmative cyber coverages clients can more closely consider the cyber peril they face and evaluate how that exposure impacts covera across their enterprise."

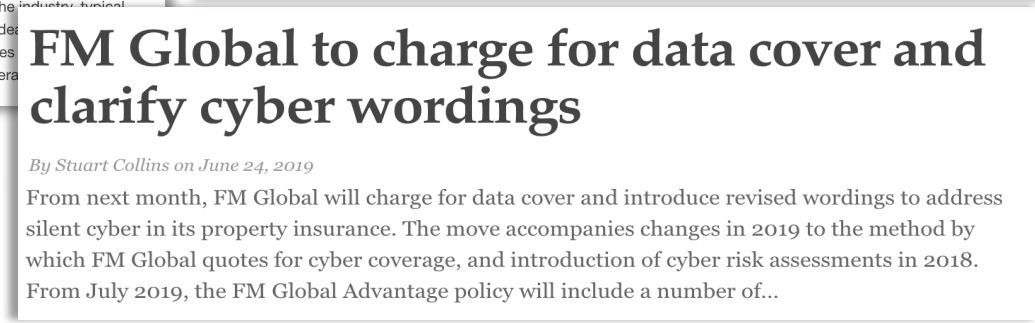


AXA XL adds first party cyber insurance option to its Platinum Property coverage

NEWS PROVIDED BY
AXA XL →
Apr 24, 2019, 10:15 ET

SHARE THIS ARTICLE

NEW YORK, April 24, 2019 /PRNewswire/ -- To help businesses in the US address business interruption resulting from a cyber attack, AXA XL, a division of AXA, has designed a first-party cyber insurance option for its Platinum Property clients -- businesses that buy 100% of their property coverage from AXA XL.



FM Global to charge for data cover and clarify cyber wordings

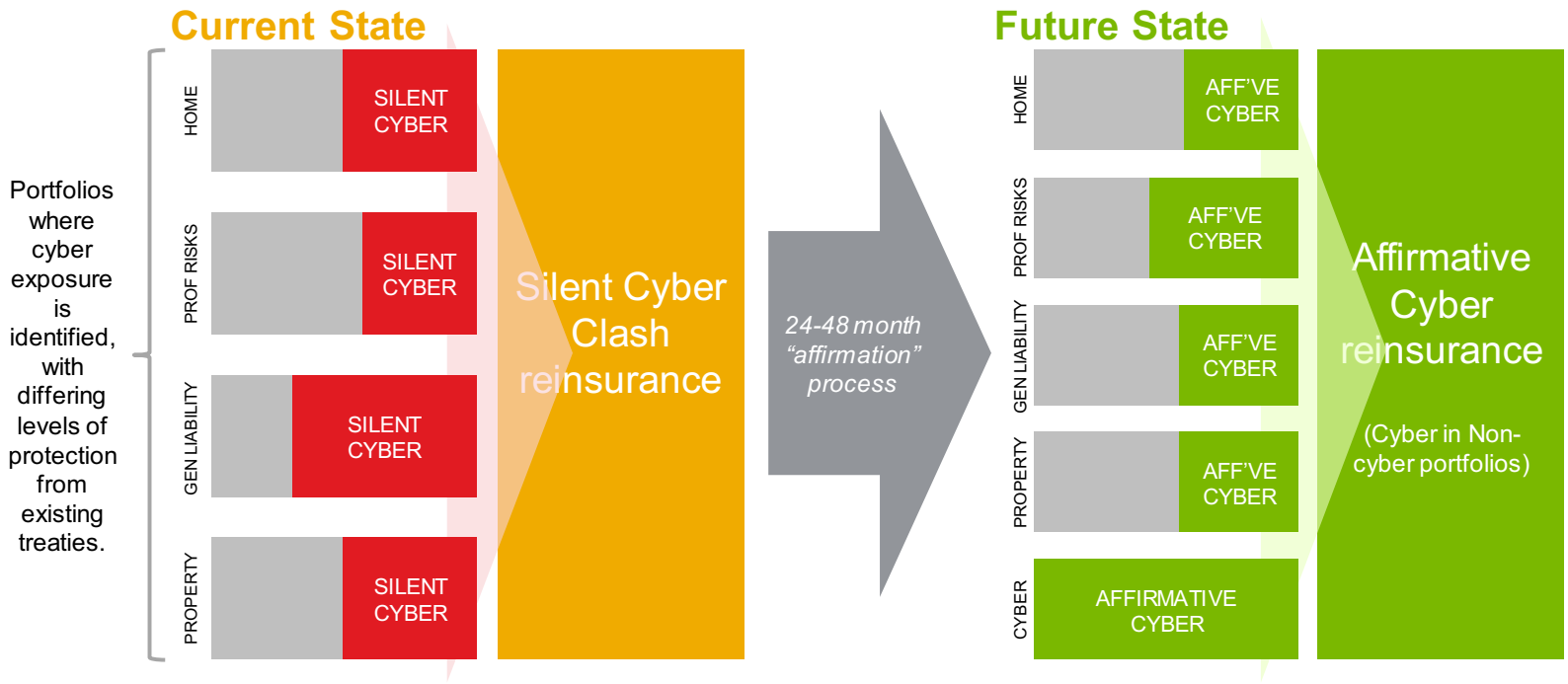
By Stuart Collins on June 24, 2019

From next month, FM Global will charge for data cover and introduce revised wordings to address silent cyber in its property insurance. The move accompanies changes in 2019 to the method by which FM Global quotes for cyber coverage, and introduction of cyber risk assessments in 2018. From July 2019, the FM Global Advantage policy will include a number of...

GUIDEWIRE CYENCE

AON Empower Results®

Transferring silent cyber risk, moving to affirmative …



GUIDEWIRE CYENCE

AON Empower Results®


Q&A

Contacts

Jon Laux, FCAS
Head of Cyber Analytics
Reinsurance Solutions
Aon plc
jonathan.laux@aon.com

Ridhima Handa Kale, FCAS
Senior Product Manager
Analytics and Data Services
Guidewire – Cyence
rkale@guidewire.com

GUIDEWIRE CYENCE

AON Empower Results®