

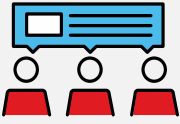
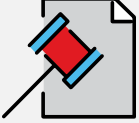


Protecting today. Safeguarding tomorrow.

*APTA Conference
Cyber Security Risk,
Mitigation, and Insurance*

February 26th, 2019

AON
Empower Results®

Aon Cyber Solutions – E&O/Cyber Broking Group

 <p>Experienced teams and resources</p>	<ul style="list-style-type: none"> ▪ Over 500 global professionals dedicated to strategy, execution, and service of errors & omissions and cyber insurance placements ▪ Product and industry expertise – Errors & omissions and cyber industry specialists aligned with Aon industry practices ▪ Policy Committee focuses on developing and enhancing policy language with clients and insurers as well as cyber product development
 <p>Market impacting solutions</p>	<ul style="list-style-type: none"> ▪ Aon Cyber Enterprise Solution® ▪ Aon's Cyber BI+ Coverage ▪ Aon's GDPR Protect Solution ▪ Aon Cyber Captive Solution ▪ Aon Client Treaty
 <p>Proprietary data and analytics</p>	<ul style="list-style-type: none"> ▪ Aon Cyber Insight loss quantification tool ▪ Aon Cyber Quotient Evaluation (CyQu) ▪ Aon Cyber Impact Analysis ▪ Aon invests \$400M in technology / data and analytics. The driving goal is to provide clients with the tools to make fact based decisions
 <p>Client engagement and expertise</p>	<p>Aon is the broker for:</p> <ul style="list-style-type: none"> ▪ 3 of the 4 world's largest cloud providers ▪ 3 of the 4 world's largest software companies ▪ 7 of the 10 world's largest technology companies ▪ 3 of the 4 world's largest content providers



Today's Discussion

- Cyber Threat Landscape
- Cyber Loss Examples
- Global Cyber Marketplace Update
- Cyber Insurance Solutions
- Q&A

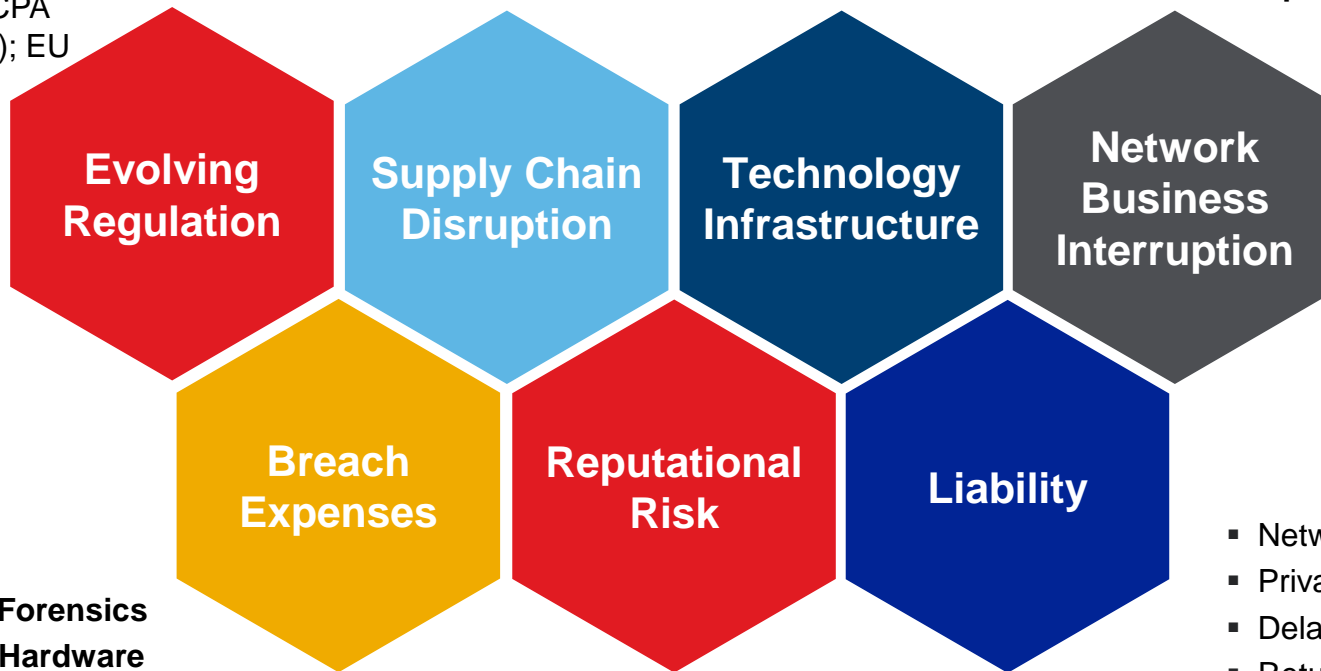
Cyber Risk Considerations for Transportation – Q1 2019

- **New cybersecurity requirements – CA IoT Law (effective 2020); NY Dept of Financial Services**
- Increasing privacy regulation – CCPA (effective 2020); EU GDPR

- Dependent & Contingent Businesses
- **Technology Dependencies**

- Information Technology Platform
- IoT / Cloud / SaaS solutions
- Operational Technology

- **Technology Failures**
- **Extended Outages caused by malicious code**
- **Logistics**
- **Net Income Loss + Extra Expense**

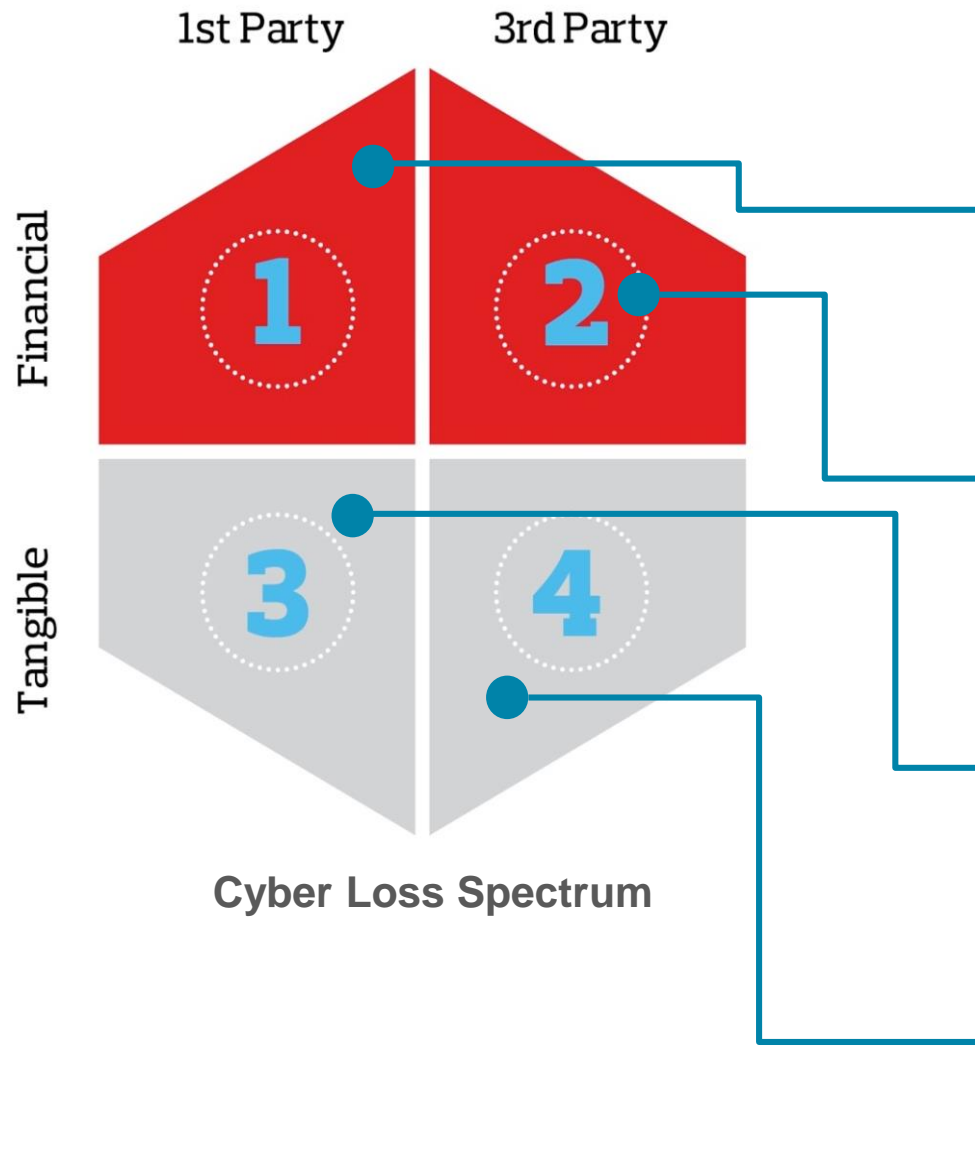


- **Computer Forensics**
- **Software / Hardware Replacement**
- **Data Restoration**
- **Notification / Credit Monitoring**

- Customer Erosion
- Public Relations Costs

- Network Security Liability
- Privacy Liability
- Delay in Delivery
- Return or Offset in Fees
- Contractual Liability / Liquidated Damages

Cyber Risk Impacts All Loss Quadrants



Any major cyber event will result in

- Public relations, response, and continuity costs
- Immediate and extended revenue loss
- Restoration expenses
- Defense costs

Third parties will seek to recover

- Civil penalties and awards
- Consequential revenue loss
- Restoration expenses

Physical damage is possible

- Property damage
- Bodily injury

Physical damage may cascade to others

- 3rd party property damage
- 3rd party bodily injury

Notable Data Breach / Privacy Commercial Impacts

Organization	Commercial Impact	Financial Components	Source
Anthem	\$278 million	Gross Expenses (\$148mm) Security Improvements (\$115mm) HIPAA Settlement (\$16mm)	Regulator Settlement U.S. District Court HHS OCR
Equifax	\$430.5 million \$514 million £500,000	Gross Expenses to Date Total Estimated Gross Expenses ICO Fine (DPA 1998)	Q3 2018 Earnings Release Q3 2018 Financials ICO Notice
Facebook	£500,000	ICO Fine (DPA 1998)	ICO Notice
The Home Depot	\$298 million	Gross Expenses	10-K Filing 2017
Target Corporation	\$292 million	Gross Expenses	10-K Filing 2017
Uber	\$148 million €400,000 €600,000 £385,000	U.S. Attorney General Settlement French CNIL Fine Dutch DPA Fine ICO Fine (DPA 1998)	U.S. AG Settlement CNIL Notice Dutch DPA Notice ICO Notice
Yahoo! Inc. (Altaba Inc.)	\$350 million \$85 million \$35 million \$80 million \$29 million £250,000	Reduced Acquisition Price Customer Class Action SEC Fine Securities Class Action Shareholder Derivative ICO Fine (DPA 1998)	Verizon Press Release U.S. District Court SEC Press Release U.S. District Court U.S. District Court ICO Notice

Notable NotPetya Business Interruption Commercial Impacts

Organization	Commercial Impact	Financial Components	Source
A.P. Moller – Maersk	\$250-300 million	Earnings Reduction	Q4 2017 Financials
Beiersdorf AG	Minimal sales impact €15 million	€35mm sales shifted Q2 to Q3 Additional expenses	Q2 2017 Financials Q4 2017 Earnings Call
FedEx (TNT Express)	\$400 million	Earnings Reduction	Q4 2018 Financials
Merck & Co.	\$410 million \$380 million	2017, 2018 Sales Reduction Additional Expenses	Q4 2017 Financials Q3 2018 Financials
Mondelez International	~\$104 million \$84 million	2017 Sales Reduction Additional Expenses	Q4 2017 Earnings Call Q4 2017 Earnings Release
Nuance Communications	\$68 million \$31.2 million	2017 Sales Reduction Additional Expenses	Q3 2018 Financials
Reckitt Benckiser	~£114 million	2% Q2 Sales Reduction 2% Q3 Sales Reduction	Press Release Q2 2017 Financials Q3 2017 Financials
Saint-Gobain	~€220-250 million €80 million	2017 Sales Reduction 2017 Earnings Reduction	Q3 2017 Earnings Release Q1 2018 Earnings Release

Notable Business Interruption Commercial Impacts

Organization	Commercial Impact	Financial Components	Source
Delta (Data Center Outage)	\$150 million	Pretax Income Reduction	Delta Industry Presentation
NHS (WannaCry)	£19 million £73 million	Lost Output IT Costs	UK Health & Social Care
TSB (IT System Failure)	£29.9 million £146.5 million	Sales Reduction Additional Expenses	Q2 Earnings Release
TSMC (Malware Outbreak)	~\$250 million	Sales Reduction	TSMC Press Release

“Silent Cyber”: Potential Cyber Perils Under P&C Policies

Property

- Hacking automated manufacturing facilities to halt production
- Inflicting bodily injury or property damage through compromised network systems
- Plant explosions or damage due to a cyber related event

Intellectual Property

- Unreleased movie / media
- Proprietary design specs for tangible and intangible assets
- Trade secrets
- Copyright materials

D&O

- Disclosures of cyber incidents have a material impact on the organizations' financial statements
- Reporting requirements
- Regulatory scrutiny

Marine

- Computerized hijacking
- Container tracking systems
- GPS navigation systems
- Automated shipyard processes



General / Product Liability

- Automated system hacking modifies product specs, creating faulty devices
- Increased products exposures to Internet of Things (“IoT”) vulnerabilities

Environmental

- Attacks on nuclear or energy facilities release hazardous chemicals or air emissions
- Untreated sewage releases to poison water supply
- Disabling of critical infrastructure leading to fires or explosions

Kidnap & Ransom

- Ransomware claims filed under K&R policies
- Social media extortion

Recall

- Hacking automated manufacturing plants
- Cyber vulnerabilities in cars and cameras
- Hacker contamination of design specs
- Nanotechnology and 3D printing

Terrorism

- Hacking medical devices to inflict bodily harm to political or public figures
- Deliberate release of misinformation to cause riot or civil unrest

Crime

- Increased sophistication of social engineering attacks
- Hacking major financial institutions or accounting software to steal monies
- Bitcoin wallet manipulation

Note that coverage in policy forms can vary materially from carrier to carrier, and from base policy forms to manuscript policy forms

Mondelez v Zurich

June 27, 2017: Mondelez affected by malicious code later dubbed NotPetya: 1700 Servers and 24,000 Laptops affected

July 18, 2018: Zurich rescinds denial – offers \$10M partial payment

October 10, 2018: Mondelez files suit for coverage for losses in excess of \$100M

June 1, 2018: Zurich formally denies Mondelez' claim based on exclusion b(2)a: War Exclusion

October 9, 2018: Zurich reasserts denial

Relevant Details:

Exclusion b(2)(a) *hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any:*

- (i) *government or sovereign power (de jure or de facto);*
- (ii) *military, naval, or air force; or*
- (iii) *agent or authority of any party specified in i or ii above.*

~\$104M earnings reduction, \$84M extra expense – 2017 Q4 Earnings Release

According to Property Claim Services (PCS) the total industry loss from the Petya / NotPetya cyber attack has now passed \$3 billion, roughly 90% of which was driven by silent cyber impacts, the remainder from affirmative losses. <https://www.reinsurancene.ws/petya-cyber-industry-loss-passes-3bn-driven-by-merck-silent-cyber-pcs/>

Sample Cyber Carve-back language: “Cyberterrorism means the premeditated use of disruptive activities against any computer system or network by an individual or group of individuals, or the explicit threat by an individual or group of individuals to use such activities, with the intention to cause harm, further social, ideological, religious, political, or similar objectives, or to intimidate any person(s) in furtherance of such objectives. ‘Cyberterrorism’ does not include any such activities which are part of or in support of any military action or war.”

Global Cyber Insurance Marketplace - 2019

DOMESTIC

- AIG
- Allianz
- Arch
- Argo
- Aspen
- At-Bay
- AXA XL
- AXIS
- AWAC
- BCS
- Beazley
- Berkley
- Berkshire Hathaway
- Cap Specialty
- Chubb
- CNA
- Coalition
- CV Starr
- Great American
- NAS
- Nationwide
- Navigators
- Hartford
- HCC
- Hiscox
- Huntersure
- Liberty/Ironshore
- MunichRe
- QBE
- RLI
- RSUI
- Safety National
- SCOR
- Sompco
- Swiss Re
- Travelers
- Validus
- Zurich

LONDON

- AIG
- Allianz
- Amlin
- Amtrust
- Argo
- Ascent
- Aspen
- Aviva
- AXA XL
- Axis
- Barbican
- Beazley
- Brit
- CFC
- Chubb
- Emergln Risk
- Hannover Re
- HCC
- HDI Gerling
- Hiscox
- Liberty
- Markel
- Munich Re
- Navigators
- Neon /Tarian
- Nirvana
- QBE
- Occam (formerly Sciemus)
- SCOR
- Swiss Re
- Talbot
- Tokio Marine Kiln
- WRB
- Zurich

BERMUDA (Excess only)

- AIG
- Arch
- AXA XL
- Chubb
- Markel
- Aspen
- AWAC
- AXIS
- Sompco
- Liberty Specialty

Cyber Market Snapshot



Claims & Losses



Coverage



Capacity



Retentions



Pricing

Stronger data is being gathered as more breaches are reported

- Complexity of breaches has driven an increase in incident response expenses incurred by Insureds
- Claims and loss data has expanded coverage offerings and improved actuarial data for loss modelling purposes
- Increasingly punitive legal and regulatory environment
- E&O Claims have been the main driver for an increase on Insurer Losses

Coverage continues to evolve and become more valuable for Insureds

- Insurers continue to update their policy forms to meet current market coverage needs
- Coverage breadth continues to expand
- Insurers continue to differentiate their offerings with new or enhanced coverage components
- Emphasis on pre-arranged vendors
- Broadening systems failure and contingent business interruption coverage solutions

Capacity is continuing to grow across geographies

- Over 75 unique Insurers providing E&O / Cyber Liability capacity
- Capacity is available the United States, London, Bermuda and Asia
- Growing number of Insurers developing appetites for large, complex risks
- There is over \$1B in theoretical capacity available in the E&O / Cyber market place

Retentions are being reviewed

- Retentions of all levels are available in the market, but can vary greatly based on industry class, size and unique exposures
- Adjusting retentions can lead to increased coverage and/or pricing flexibility

Pricing trends are competitive, but increasing for some industries

- Average premium rates reflect a decline – however dependent upon underwriting and scope of coverage
- Excess rate environment continues to be competitive
- Some Insureds have secured significant coverage improvements as a result of paying higher premiums

Note: This is a general summary and could vary based on client industry and size

Purchasing Trends by Industry

Limit increases at renewal

- Companies in a number of industries, including financial institutions, hospitality, healthcare, retail, manufacturing, technology, media and transportation, are **seeking higher limits options**
- For other industries, many organizations are still evaluating the purchase of cyber insurance or use of their captive to provide cyber cover due to regulatory, contract, D&O, benchmarking / loss information and financial statement pressures, among other reasons

More new buyers

- Manufacturing, critical infrastructure, pharmaceutical / life sciences, industrials & materials / automotive, public sector, energy / power and utilities, higher education, real estate / construction, agribusiness and transportation / logistics industries saw the biggest uptick in new cyber insurance purchases in 2018
- Major concern in these industries is **business interruption loss and reliance on technology**

Shifting focus on cyber risk exposures

- In prior years, organizations' primary cyber concern was related to privacy breaches
- In 2018, more clients across all industries have focused on **business interruption coverage, including system failure cover, cyber extortion and digital asset restoration**
- Cyber insurance cases where courts upheld denial of coverage demonstrate the critical importance of **matching customized policy wording to specific insured cyber exposures**

Market Standard Cyber Coverages Overview



- Network Business Interruption
- System Failure
- Dependent Business Interruption / System Failure
- Cyber Extortion
- Digital Asset Restoration



- Privacy and Network Security Liability
- Privacy Regulatory Fines and Penalties
- Media Liability
- PCI Fines and Penalties
- Breach Event Expenses

Scope of Cyber Insurance Coverage



- **Network Business Interruption** - Reimbursement coverage for the insured for lost net income caused by a network security failure, as well as associated extra expense. Retention and waiting periods are negotiable
- **System Failure** - Expands coverage trigger for business interruption beyond computer network security failure to include any system failure
- **Dependent Business Interruption/Dependent System Failure** - Reimbursement coverage for the insured for lost income caused by a network security failure of a business on which the insured is dependent, as well as associated extra expense. Retentions and waiting periods are negotiable.
- **Cyber Extortion** - Reimbursement coverage for the insured for expenses incurred in the investigation of a threat and any extortion payments made to prevent or resolve the threat.
- **Digital Asset Restoration** - Reimbursement coverage for the insured for costs incurred to restore, recollect, or recreate intangible, non-physical assets (software or data) that are corrupted, destroyed or deleted due to a network security failure

Scope of Cyber Insurance Coverage



- **Privacy and Network Security Liability –**
 - **Privacy Liability:** Liability coverage for defense costs and damages suffered by others for any failure to protect personally identifiable or confidential third-party corporate information, whether or not due to a failure of network security. Coverage may include: unintentional violations of the insured's privacy policy, actions of rogue employees, and alleged wrongful collection of confidential
 - **Security Liability:** Liability coverage for defense costs and damages suffered by others resulting from a failure of computer security, including liability caused by theft or disclosure of confidential information, unauthorized access, unauthorized use, denial of service attack or transmission of a computer virus
- **Privacy Regulatory Fines and Penalties -** Liability coverage for defense costs for proceedings brought by a governmental agency in connection with a failure to protect private information and/or a failure of network security. Coverage includes fines and penalties where insurable by law. Compensatory damages, i.e. amounts the insured is required by a regulator to deposit into a consumer redress fund, may be covered
- **Media Liability -** Liability coverage for defense costs and damages suffered by others for content-based injuries such as libel, slander, defamation, copyright infringement, trademark infringement, or invasion of privacy. The scope of covered media is variable and can range from the insured's website only to all content in any medium
- **PCI Fines and Penalties -** Coverage for a monetary assessment (including a contractual fine or penalty) from a Payment Card Association (e.g., MasterCard, Visa, American Express) or bank processing payment card transactions (i.e., an "Acquiring Bank") in connection with an Insured's non-compliance with PCI Data Security Standards
- **Breach Event Expenses -** Reimbursement coverage for the insured's costs to respond to a data privacy or security incident. Policy triggers vary but are typically based on discovery of an event, or a statutory obligation to notify consumers of an event. Covered expenses include computer forensics expenses, legal expenses, costs for a public relations firm and related advertising to restore your reputation, consumer notification, call centers, and consumer credit monitoring services

Questions?

About Cyber Solutions

Aon's Cyber Solutions offers holistic cyber risk management, unsurpassed investigative skills, and proprietary technologies to help clients uncover and quantify cyber risks, protect critical assets, and recover from cyber incidents.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

Visit aon.com/cyber-solutions for more information.
© Aon plc 2019. All rights reserved.

Cyber security services offered by Stroz Friedberg Inc. and its affiliates. Insurance products and services offered by Aon Risk Insurance Services West, Inc., Aon Risk Services Central, Inc., Aon Risk Services Northeast, Inc., Aon Risk Services Southwest, Inc., and Aon Risk Services, Inc. of Florida and their licensed affiliates.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.