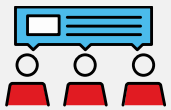
Cyber Development

Presentation Date: May 10, 2017

Aon Risk Solutions
Professional Risk Solutions

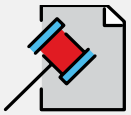
Empower Results®

Aon's Professional Risk Solutions Group



Experienced teams and resources

- **Over 60 U.S. professionals** dedicated to strategy, execution, and service
- **Product and industry expertise** - Cyber industry specialists aligned with Aon industry practices
- **Policy Committee** focuses on developing policy language with clients and Insurers as well as cyber product development



Market impacting solutions

- **Aon Cyber Enterprise Solution™**, a first-of-its-kind property / casualty and Internet of Things insurance policy that offers comprehensive and integrated enterprise-wide coverage against cyber risk
- **EU Data Protect**
- **Cyber Captive Solution**

Proprietary data and analytics

- **Cyber Insight** actuarial review
- **Aon Cyber 360** Suite of Solutions
- **Aon Cyber Impact Analysis / Risk Financing Decision Platform**

Industry leading talent

- 2016 appointment of **James Trainor** as Senior Vice President of the Cyber Solutions Group. Mr. Trainor joins Aon after a distinguished career at the FBI, where he most recently led the Cyber Division

Strategic acquisition

- On November 1, 2016, Aon finalized its acquisition of cyber risk consulting firm **Stroz Friedberg**
- Aon's union with Stroz Friedberg provides a comprehensive suite of assessment and quantification solutions to support our clients

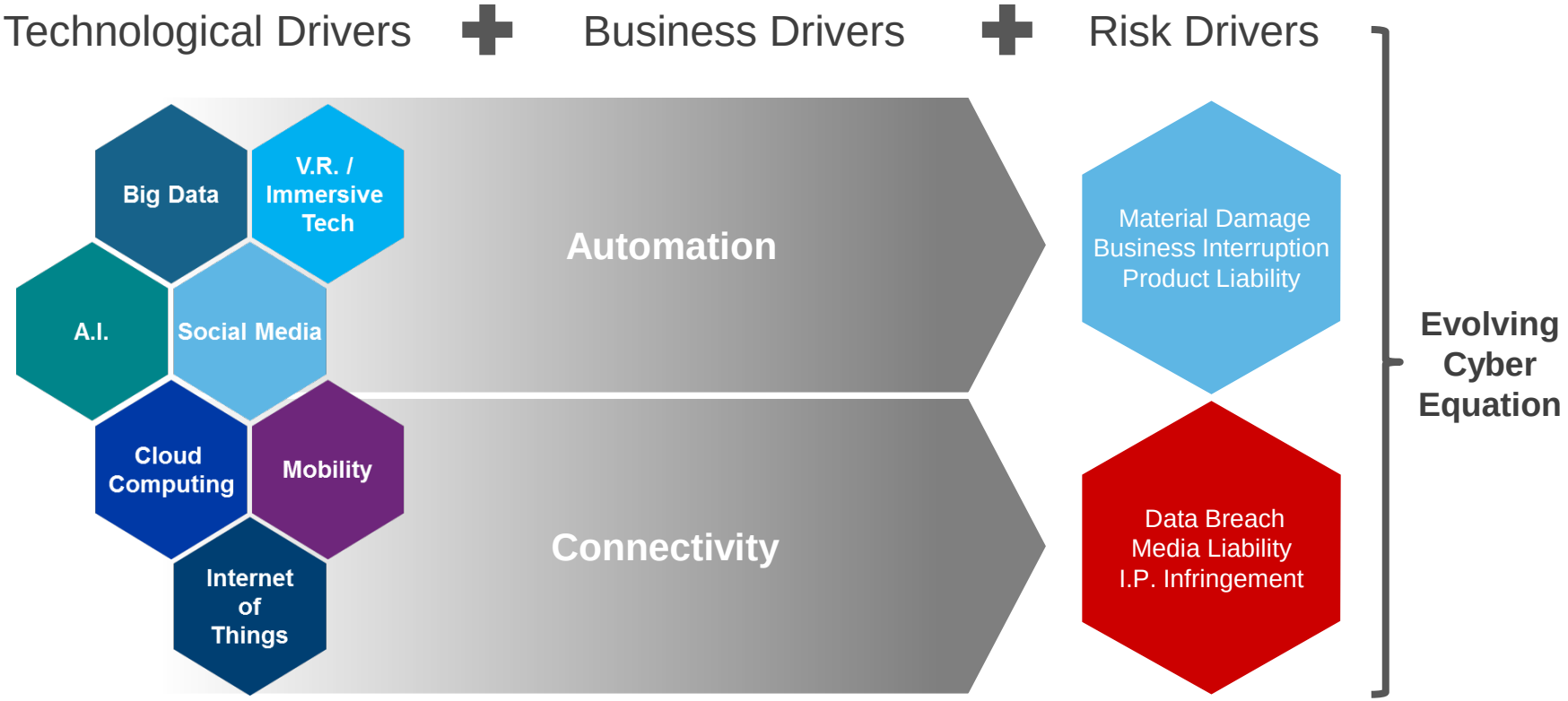
$400M+
in total premium placed in 2016

60+
Global Professionals

500+
cyber claims managed by Aon since 2012

The Evolving Cyber Threat

Across all industries, our clients are continuing to invest in deploying digital technologies to stay competitive and drive quality and efficiency objectives



2017 Cyber Exposure Trends

IoT - The Internet of Things
Reliance on technology & increasing connectivity

Cloud Computing / Big Data Analytics
Increased use of technology vendors

Social Media
Social Engineering
Phishing / Spear Phishing

Ransomware / Malware / Cyber Heist / Blockchain

U.S. and International Regulatory Environment
EU General Data Protection Regulation – effective May 25, 2018

Stroz Friedberg – Top Cyber Risks in 2017

1. **Criminals harness IoT devices as botnets to attack infrastructure**: In 2017, Stroz Friedberg predicts there will be an increase in IoT devices compromised, harnessed as botnets, and used as launching points for malware propagation, SPAM, DDoS attacks and anonymizing malicious activities.

2. **Nation state cyber espionage and information war influences global and political policy**: Cyber espionage will continue to influence global politics and will spread to the upcoming elections in Latin America and Europe. Russia, China, Iran, and North Korea will be regions of great concern in 2017, as they continue to develop deep pools of cyber-crime talent.

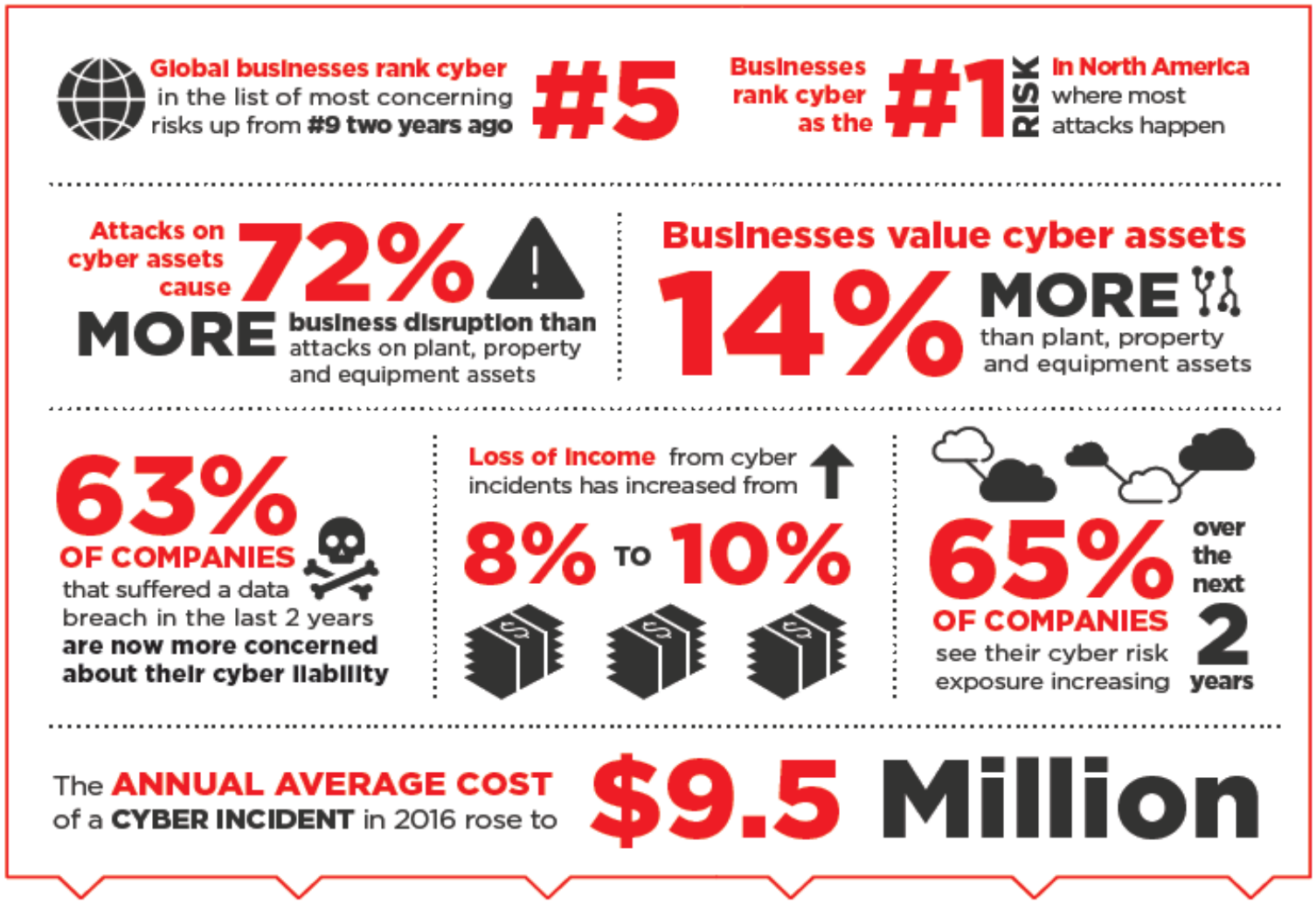
3. **Data integrity attacks rise**: Data sabotage as the next big threat will become a reality in 2017. Criminals will seek to sow confusion and doubt over the accuracy and reliability of information, impairing decision-making across the private and public sector.

4. **Spear-phishing and social engineering tactics**: In 2017, advanced social engineering tactics will become more targeted, cunning, and more effective, exploiting the weakest link – employees – that organizations always find challenging to safeguard.

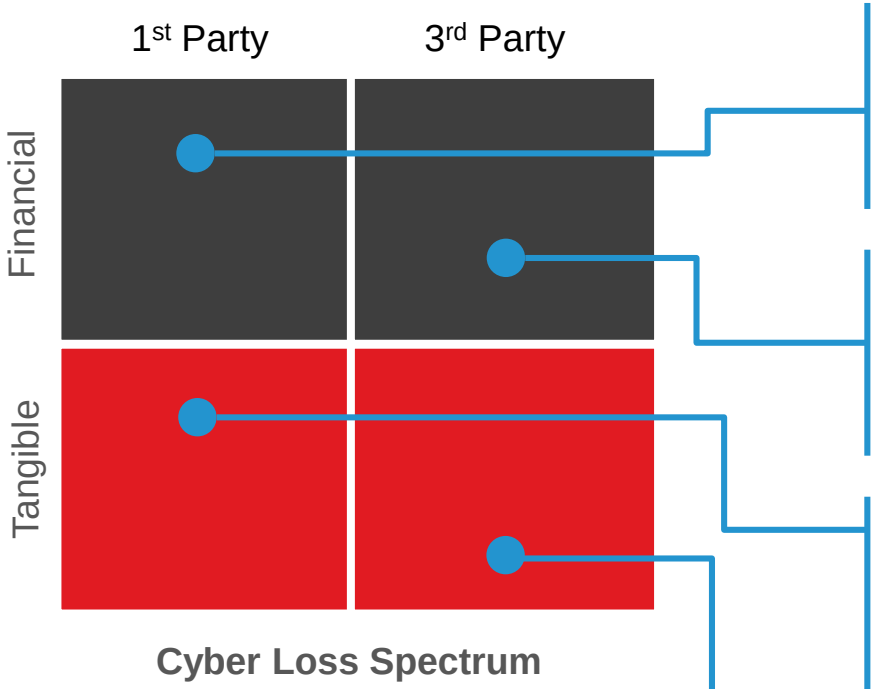
5. **Red teaming and cybersecurity talent development**: Increased pressure from regulators worldwide will push in-house red teaming capabilities to accelerate in 2017. In addition, companies that are not in the cyber business will face a different challenge: recruiting, motivating, and retaining highly technical cyber talent to keep their red teams at the forefront of cybersecurity.

6. **Pre-M&A cybersecurity due diligence**: The financial services industry will be early-adopters of making cybersecurity due diligence a critical part of the pre-M&A due diligence process. While 2017 will see one to two additional high profile instances that impact the M&A deal process outcome, only the financial services industry will react accordingly and conduct judicious cyber assessments.

Cyber Risk Is Top Concern of Companies



Cyber Risk Impacts All Loss Quadrants



Any major cyber event will result in

- PR, 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

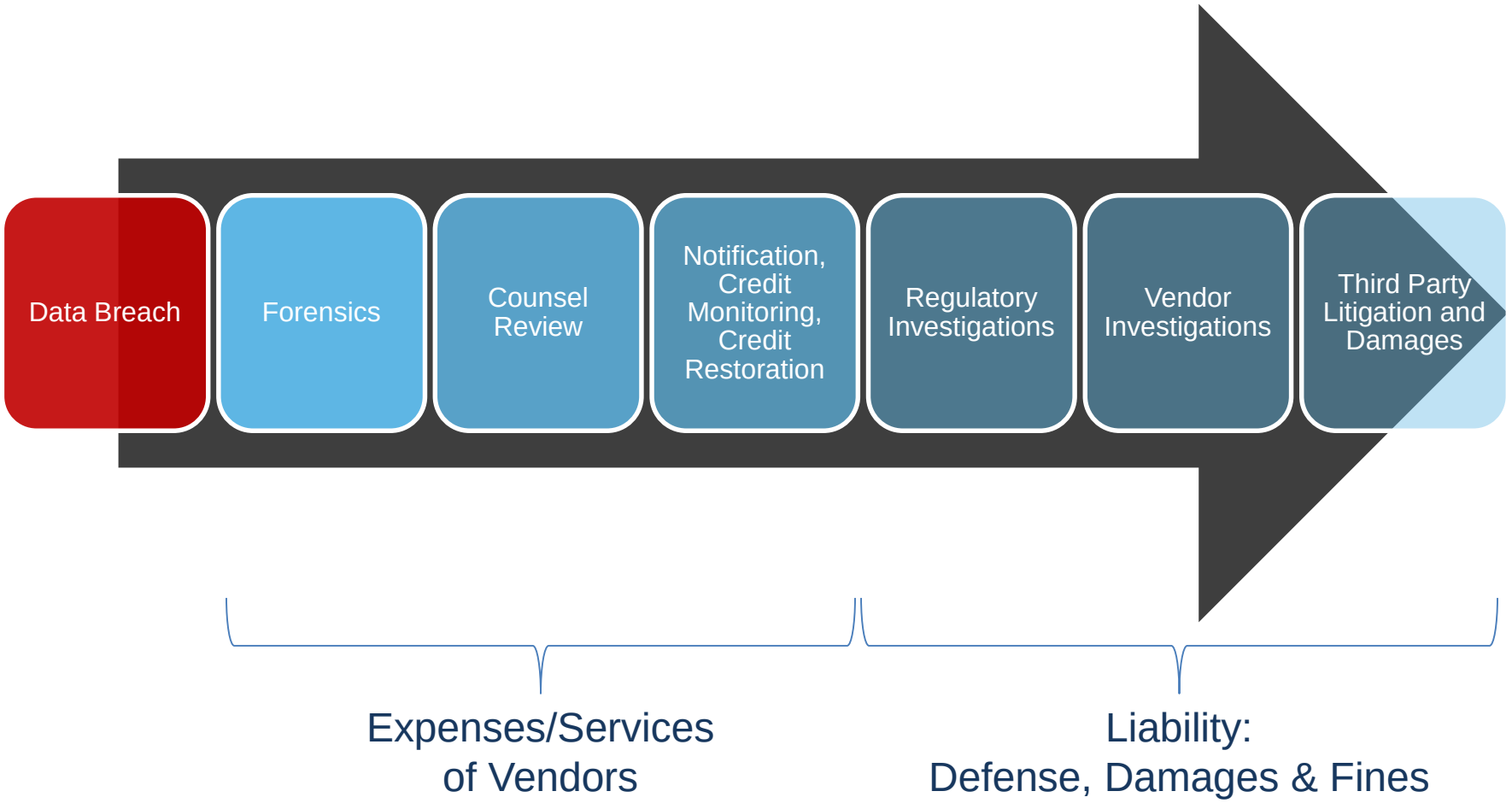
Physical damage is possible

- Property damage
- Bodily injury

Physical damage may cascade to others

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

Traditional Information Release Event



Scope of Cyber Insurance Coverage

Defense Costs + Damages + Regulator Fines	Insured's Loss	Expenses Paid to Vendors
Liability Sections ▪ Failure of Network Security ▪ Failure to Protect / Wrongful Disclosure of Information, including employee information ▪ Privacy or Security related regulator investigation ▪ All of the above when committed by an outsourcer ▪ Wrongful Collection of Information (some policies) ▪ Media content infringement / defamatory content	**First Party Sections** ▪ Network-related Business Interruption ▪ Extra Expense ▪ System Failure Business Interruption (some policies) ▪ Dependent Business Interruption (some policies) ▪ Intangible Asset damage	**Expense / Service Sections** ▪ Crisis Management ▪ Breach-related Legal Advice ▪ Call Center ▪ Credit Monitoring, Identity Monitoring, ID Theft Insurance ▪ Cyber Extortion Payments

Aon Cyber Enterprise Solution™

Cyber risk = Enterprise risk

Cyber risk transfer solutions need to address evolving exposures:

- Business Interruption
- Property damage
- Internet of Things liability
- Supply Chain exposure
- Vendors, including Cloud
- Regulatory

Aon Cyber Enterprise Solution™ addresses emerging areas of cyber risk and related regulation including:

- Property damage arising out of a network security breach
- Products liability coverage to address Internet of Things exposures
- Business interruption and extra expense coverage arising out of a systems failure
- Contingent network business interruption for IT vendors and the supply chain
- Cyber terrorism coverage
- European Union General Data Protection Regulation (effective May 25, 2018) fines and penalties, where insurable
- Privacy / security liability and event expense coverage
- Media liability and technology errors and omissions by endorsement

The Aon Approach:

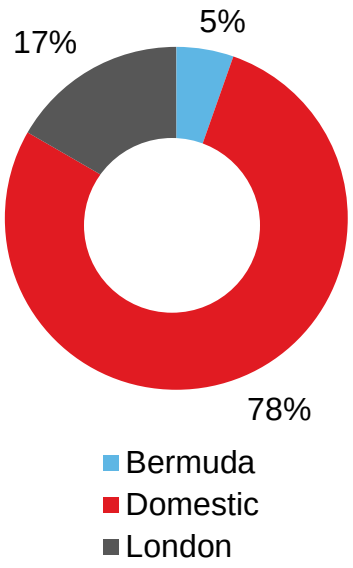
- Comprehensive limit – up to USD 400 million in capacity
- Aon proprietary language – single policy form
- Coverage is primary over any other valid and collectable insurance
- Potential captive utility

Cyber State of the Marketplace

Capacity is continuing to grow across geographies	Coverage continues to evolve and become more valuable	Stronger data is being gathered as more breaches are reported	Retentions have stabilized since 2015 pressures	Primary pricing trends are beginning to decline, with excess trends softening
▪ Over 65 unique Insurers providing E&O / Cyber Liability capacity ▪ Capacity is available domestically (primary and excess), in the U.K. (primary and excess) and in Bermuda (excess only, generally attaching above $50M) ▪ There is over $700M in theoretical capacity available in the E&O/Cyber market place	▪ Coverage breadth and limit availability continues to expand ▪ Insurers continue to differentiate their offerings with new or enhanced coverage components ▪ Breach response coverage continues to increase and expand to meet Insured's needs ▪ Insurers continue to build out pre breach offerings as part of their policy package	▪ Increased ransomeware activity and business interruption concerns ▪ Claims and loss data has expanded coverage offerings and improved actuarial data for loss modeling purposes ▪ Increasingly punitive legal and regulatory environment ▪ Open privacy-related litigation can take years to conclude	▪ 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 increase flexibility in limits and pricing	▪ Depending on loss history and claims experience, pricing has begun to stabilize due to large readjustments that took place in prior years ▪ Renewal premiums are falling in line with the change in exposure levels ▪ Excess rate environment has been softening

Global Cyber Insurance Marketplace

Aon Client Premium Spend



DOMESTIC

- AIG
- Allianz
- Arch
- Argo
- Aspen
- AXIS
- AWAC
- BCS
- Beazley
- Berkshire Hathaway
- Chubb
- CNA
- CV Starr
- Endurance
- Nationwide
- Hartford
- HCC
- Hiscox
- Ironshore
- Liberty Mutual
- QBE
- RLI
- RSUI
- SCOR Re
- Swiss Re
- Travelers
- XL- Catlin
- Zurich

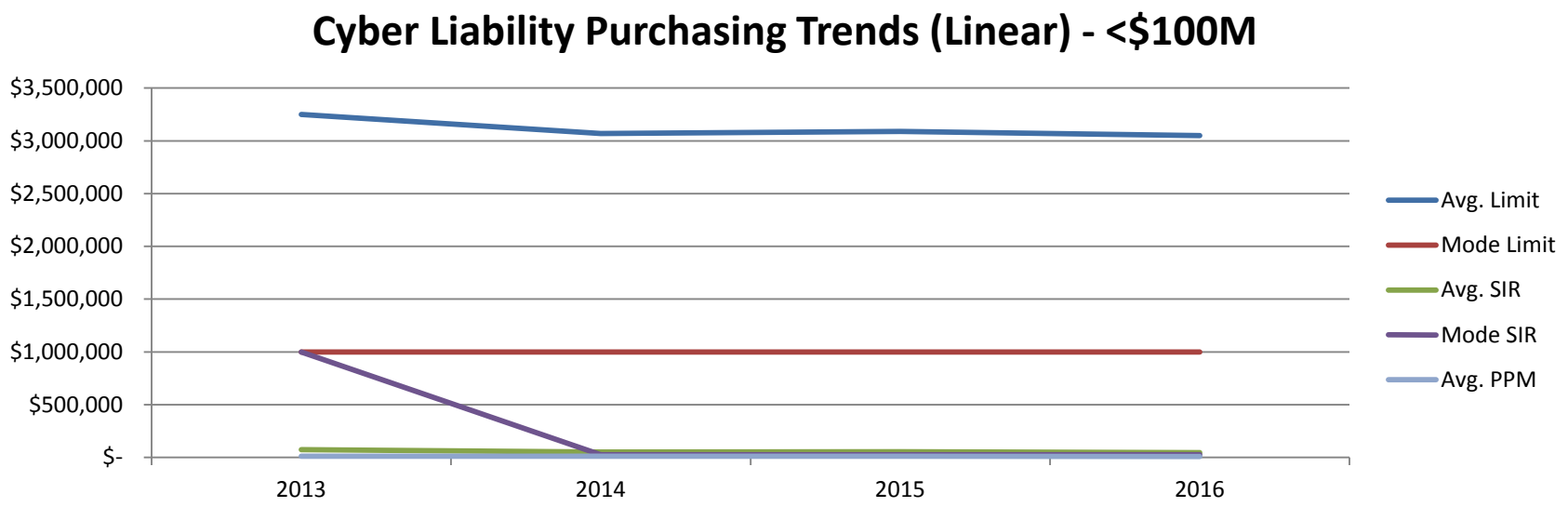
LONDON

- ANV
- Ascent
- Aspen
- AIG
- Axis
- Barbican
- Beazley
- Brit
- CFC
- Chubb
- Emerging Risks
- Hannover Re
- HCC
- HDI Gerling
- Hiscox
- Kiln
- Liberty
- Markel
- Munich Re
- Novae
- Principia
- Sceimus
- SCOR
- Swiss Re
- Talbot
- Zurich

BERMUDA (Excess only)

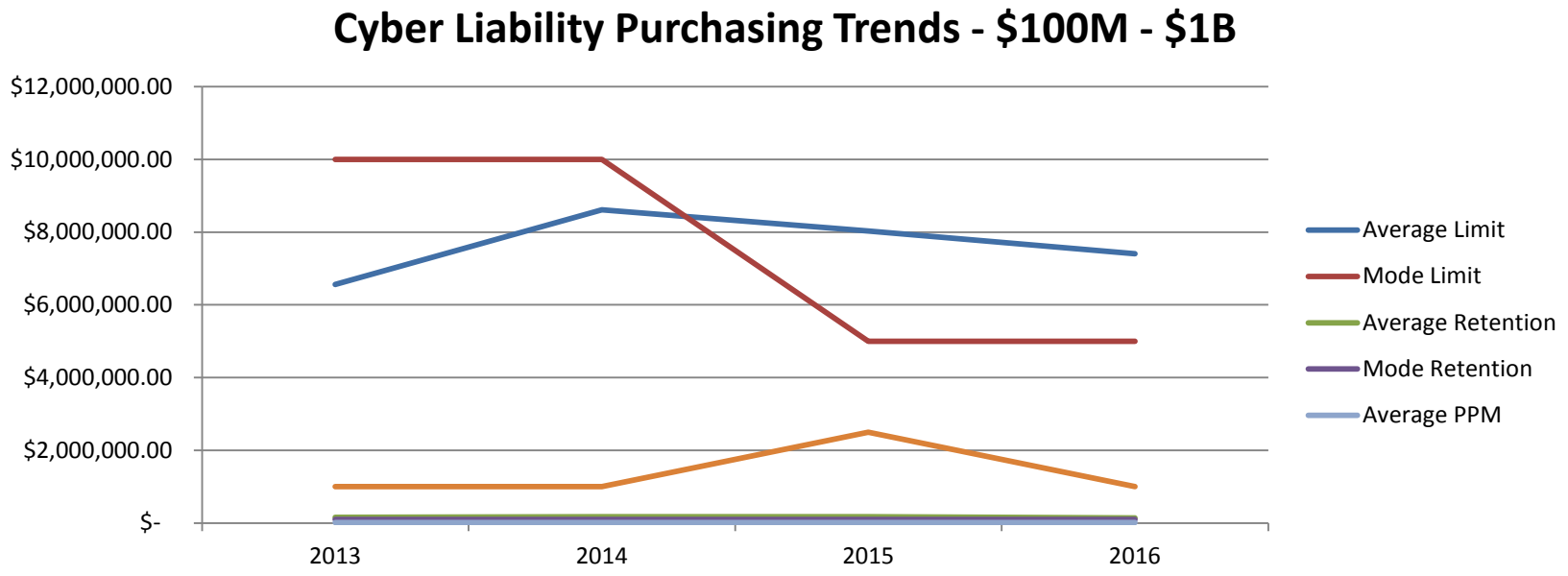
- AIG
- Chubb
- Markel
- Argo
- Aspen
- AWAC
- AXIS
- Endurance
- Iron-Starr
- XL - Catlin

Purchasing Trends



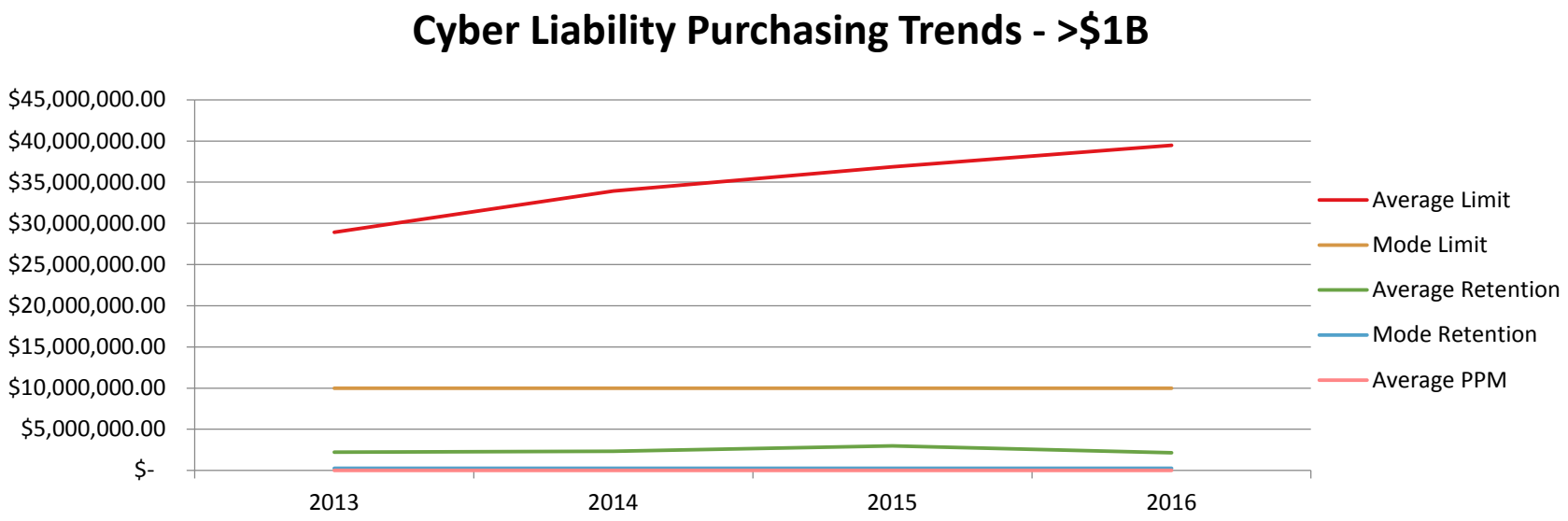
	Avg. Limit	Mode Limit	Avg. SIR	Mode SIR	Max Limit	Max SIR	Avg. PPM
2013	$ 3,250,000.00	$ 1,000,000.00	$ 74,545.00	$ 1,000,000.00	$ 50,000,000.00	$ 750,000.00	$ 12,266.67
2014	$ 3,068,611.11	$ 1,000,000.00	$ 50,080.56	$ 25,000.00	$ 20,000,000.00	$ 500,000.00	$ 10,314.44
2015	$ 3,090,298.51	$ 1,000,000.00	$ 54,535.45	$ 25,000.00	$ 40,000,000.00	$ 500,000.00	$ 9,860.82
2016	$ 3,048,338.37	$ 1,000,000.00	$ 44,995.47	$ 25,000.00	$ 50,000,000.00	$ 1,000,000.00	$ 8,771.90

Purchasing Trends



	Average Limit	Mode Limit	Average Retention	Mode Retention	Max Limit	Max SIR	Average PPM
2013	$ 6,562,500.00	$ 10,000,000.00	$ 154,062.50	$ 100,000.00	$ 40,000,000.00	$ 1,000,000.00	$ 16,201.56
2014	$ 8,613,496.93	$ 10,000,000.00	$ 175,245.40	$ 100,000.00	$ 150,000,000.00	$ 1,000,000.00	$ 14,869.94
2015	$ 8,030,075.19	$ 5,000,000.00	$ 169,132.08	$ 100,000.00	$ 150,000,000.00	$ 2,500,000.00	$ 13,960.15
2016	$ 7,404,696.13	$ 5,000,000.00	$ 136,705.80	$ 100,000.00	$ 160,000,000.00	$ 1,000,000.00	$ 13,277.07

Purchasing Trends



	Average Limit	Mode Limit	Average Retention	Mode Retention	Max Limit	Max SIR	Average PPM
2013	$ 28,918,478.26	$ 10,000,000.00	$ 2,223,913.04	$ 250,000.00	$ 250,000,000.00	$ 25,000,000.00	$ 21,093.48
2014	$ 33,908,450.70	$ 10,000,000.00	$ 2,331,914.89	$ 250,000.00	$ 300,000,000.00	$ 50,000,000.00	$ 24,775.35
2015	$ 36,869,897.96	$ 10,000,000.00	$ 2,981,045.92	$ 250,000.00	$ 400,000,000.00	$ 200,000,000.00	$ 25,822.96
2016	$ 39,481,092.44	$ 10,000,000.00	$ 2,152,794.13	$ 250,000.00	$ 500,000,000.00	$ 1,000,000.00	$ 26,629.83

Cyber Purchasing Trends – Q1 2017

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, higher education, real estate/construction, agribusiness and transportation/logistics industries saw the biggest uptick in new cyber insurance purchases in 2016
- 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 2016, more clients across all industries have focused on business interruption coverage, including systems 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 match specific insured cyber exposures

Cyber Purchasing Trends by Geography – Q1 2017

Global growth in cyber insurance

- 25%-35% year over year growth of United States Cyber insurance premium
- United States small and middle market growth in excess of 35%
- New business growth in Europe, the Middle East and Africa, as well as Australia, due to the development of privacy regulation
- European Union General Data Privacy Regulation (effective May 2018) contains fines of up to 4% of an organization's worldwide revenue/turnover
- Latin America and Asia becoming more active in terms of inquiries for Cyber insurance

Selected Data Breach Incidents: 2013 – 2014

Date	Company	Incident	Severity	Estimated Cost/Loss
August 2013	Toyota/Ford	White hat demo hack of Toyota Prius and Ford Escape to wrest control of breaks, steering, and acceleration	N/A	N/A
December 2013	Target Corp.	Attacker leveraged access to a third party network of Target's	110M individuals affected	$291M+
January 2014	Neiman Marcus	A customer information database was hacked	1.2M individuals affected	$147.2M
January 2014	Michaels Stores Inc.	Point-of-sale (POS) malware	3M individuals affected	TBD
February 2014	Wyndham Worldwide	Intruders gained unauthorized access to Wyndham's computer network	619,000 individuals affected	$10M+
July 2014	JPMorgan Chase	System was hacked	83M accounts and 7M small businesses affected	Est. $250M spent on cybersecurity
September 2014	Home Depot	Massive breach of credit card information for an intrusion first reported in April of 2014	56M individuals affected	$232M+
November 2014	Sony Pictures	Cyber extortion and hack potentially related to the release of "The Interview"	47,000 SSN information stolen	$15M+
December 2014	Staples	Cyber criminals stole customer card data from a subset of Staples locations	1.16M individuals affected	TBD
December 2014	German Steel Mill	Massive physical damage to plant arising out of malware on system	Not disclosed	TBD

Selected Data Breach Incidents: 2015

Date	Company	Incident	Severity	Estimated Cost/Loss
February 2015	Anthem, Inc.	Information technology system hacked	80M individuals affected	$100M+
May 2015	IRS website	Criminals used stolen data to file fraudulent tax returns	100K people affected	$50M
June 2015	Office of Personnel Management	Hacker stole government data	21.5M records stolen	$133M+
June 2015	Samsung	Discovery that every Samsung Galaxy device has a significant flaw that lets allows hackers access	600M Samsun Galaxy phones	TBD
July 2015	Ashley Madison	Users' data was stolen and threatened to be released	32M site members >60 gigabytes of data	TBD
July 2015	Fiat Chrysler	Recall over a vulnerability in dashboard computers	1.4M vehicles	TBD
July 2015	General Motors	White hat hackers broke into GM OnStar system	N/A	N/A
August 2015	Tesla	White hat hackers implanted malware into the car's central computer	Patch of car computer software required	N/A
October 2015	T-Mobile	Data breach at financial credit processing firm Experian	15M individuals affected	TBD
December 2015	Ukraine Power Grid	Hackers implant operation-specific malicious firmware with coordinated DDoS attack against customer call centers	230,000 left without power for 6 hours	Unknown

Selected Data Breach Incidents: 2016

Date	Company	Incident	Severity	Estimated Cost/Loss
February 2016	Bank of Bangladesh	Hackers used malware to obtain credentials of banks employees and sent more than three dozen fraudulent money transfer requests	At least two banks	$81M
February 2016	Hollywood Presbyterian	Ransomware attack - Hacker seized control of hospital's computer systems and would only give back access if the ransom was paid	3 days to regain control of system	$17,000 ransom plus unreported business interruption costs
April 2016	Mossack Fonseca (The Panama Papers)	11.5 million confidential documents (2.6 TB of data) containing information on >214,000 offshore companies. Anonymous source made data available in batches to German newspaper Süddeutsche Zeitung beginning in early 2015	11.5M confidential documents	TBD
July 2016	Blue Cross Blue Shield Kansas City	Data breach included names, addresses, and some plan information	790,000 members	TBD
August 2016	Delta	Three day computer failure due to technology problems	2,000 flights canceled	$150M
September 2016	Yahoo	In 2014, a state-sponsored actor accessed personal account information and in some cases, security questions and answers, making it amongst the largest breach of a single site in history	500 million user accounts	TBD
October 2016	Dyn	Hackers distributed Malware on 100,000+ IoT devices in a coordinated DDoS attack. Service was halted to major retailers like Netflix, Twitter, Spotify, and other popular websites in the US and Europe.	TBD	$110M+ in lost revenue of impacted clients

Selected Data Breach Incidents: 2016

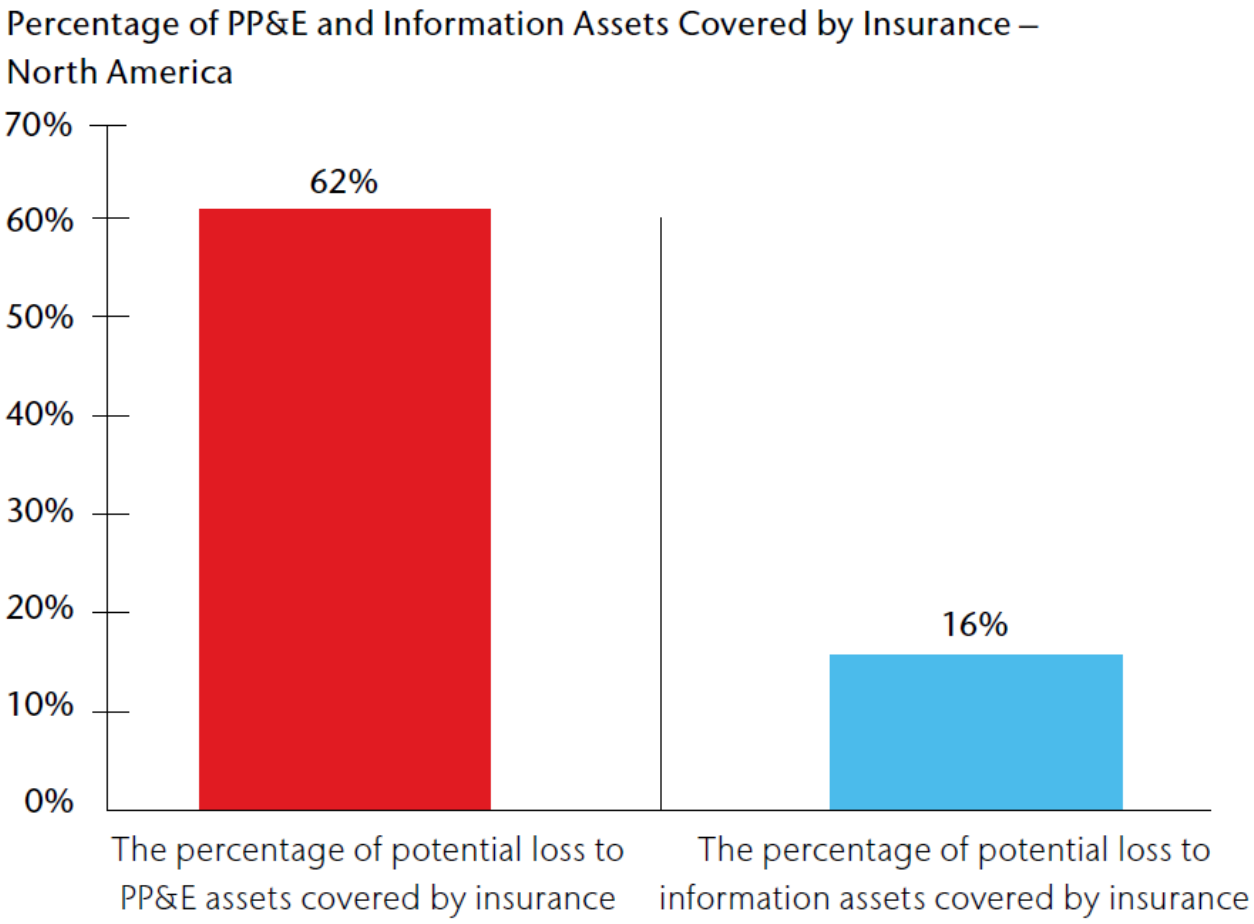
Date	Company	Incident	Severity	Estimated Cost/Loss
November 2016	Michigan State University	Unauthorized access to records exposed students and staff member's personal data. Hackers emailed an extortion demand to university personnel, who turned the matter over to local law enforcement.	400,000 records	$3M+
November 2016	San Francisco Municipal Transportation Agency	A phishing email allowed the download of a malware which infected kiosks. Hackers issued a ransom demand for 100 Bitcoins ($73,000) claiming they had more than 30GB of personal information of employees and riders.	TBD	SFMTA provided 2 days of free rides

2016 Aon Captive Cyber Benchmarking Survey

Topics	Data Holders	Product Risk	Critical Infrastructure	Transportation	Heavy Industry
Top Cyber Risk Concern	Post Breach Business Interruption	Business Interruption	Business Interruption	Business Interruption	Business Interruption
Lowest Cyber Risk Concern	Bodily Injury/ Property Damage	Bodily Injury/ Property Damage	Data & System Restoration	Loss of IP	Bodily Injury/ Property Damage
Use of Risk Assessment to inform Coverage/limits	51%	75%	59%	70%	56%
Rationale for buying cover	Board Due Diligence (80%)	Balance Sheet Protection (58%)	Balance Sheet Protection (71%)	Balance Sheet Protection (64%)	Board Due Diligence (56%)
Who is buying	70%	17%	29%	33%	33%
Limits (m)	USD 10-25	USD 10-25	>USD 100	USD 10-25	USD 10-25
Budgeted for Cyber Cover	74%	31%	41%	9%	33%

Source: 2016 Aon Captive Cyber Benchmarking Survey by Industry
Cyber—The Fast Moving Target: Benchmarking views and attitudes by industry: http://www.aon.com/risk-services/cyber.jsp

2017 Aon/Ponemon Cyber Risk Transfer Comparison Report



- The impact of business disruption to cyber assets is 72% greater than to property, plant and equipment assets
- Nearly 65% of organization expect their cyber risk exposure to increase in the next two years
- Organization value cyber assets 14% more than property, plant and equipment

How Does Analytics Change the Decision Making Process?

Aon Cyber Insight Model

- Analytic model based on privacy loss
- Loss severity analysis with breakdown of first and third party losses

Risk Financing Decision Platform

- Actuarial analysis that builds upon the Cyber Insight Model to include network business interruption

Aon Cyber 360

- Cyber risk assessment tool focusing on information assets, cyber threats, and control weaknesses to identify the level of organizational cyber exposure. Cyber 360 benchmarks controls against a hybrid of best practice and standards (i.e. ISO 27002, NIST, SANS 20) to identify strengths, improve weaknesses and define improvement recommendations.
- Bolt on quant models such as **Aon Cyber Impact Analysis** (probable maximum loss / Volatility Study) available based on individual client need

About Aon

Aon plc (NYSE:AON) is the leading global provider of risk management, insurance and reinsurance brokerage, and human resources solutions and outsourcing services. Through its more than 66,000 colleagues worldwide,

Aon unites to empower results for clients in over 120 countries via innovative and effective risk and people solutions and through industry-leading global resources and technical expertise. Aon has been named repeatedly as the world's best broker, best insurance intermediary, best reinsurance intermediary, best captives manager, and best employee benefits consulting firm by multiple industry sources.

Visit aon.com for more information on Aon.

www.aon.com

Risk. Reinsurance. Human Resources.

Empower Results®